

# User Guide

## FortiNDR Cloud



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



April 10, 2024

FortiNDR Cloud User Guide

78-281-880837-20240410

# TABLE OF CONTENTS

|   |           |
|---|-----------|
| <b>Change Log</b> .....                         | <b>7</b>  |
| <b>Overview</b> .....                           | <b>8</b>  |
| Getting started .....                           | 8         |
| Portal navigation .....                         | 9         |
| Network Entity .....                            | 9         |
| Network events .....                            | 10        |
| Event types and fields .....                    | 11        |
| Event types .....                               | 11        |
| Field types .....                               | 12        |
| Enriched object field types .....               | 13        |
| Common fields .....                             | 17        |
| Event fields .....                              | 18        |
| IQL Quick Reference .....                       | 42        |
| Network Security Posture Examples .....         | 42        |
| Hunt Examples .....                             | 44        |
| Events and Properties .....                     | 45        |
| Property Comparisons .....                      | 46        |
| Querying Array/Nested Fields .....              | 47        |
| Building Complex Queries .....                  | 48        |
| Aggregations .....                              | 48        |
| Key terms and concepts .....                    | 49        |
| <b>Dashboard</b> .....                          | <b>51</b> |
| Default dashboard .....                         | 51        |
| Observation detail page .....                   | 52        |
| MITRE ATT&CK .....                              | 54        |
| Viewing the MITRE ATT&CK Matrix .....           | 55        |
| Creating custom dashboards .....                | 56        |
| <b>Detections</b> .....                         | <b>59</b> |
| Rule Categories .....                           | 61        |
| Triage rules .....                              | 62        |
| Adding custom filters to a rule signature ..... | 65        |
| Muting rules .....                              | 66        |
| Muting a device for an account .....            | 68        |
| Excluding devices .....                         | 69        |
| Disabling rules .....                           | 69        |
| Resolving detections .....                      | 70        |
| Creating a rule .....                           | 71        |
| Start an investigation .....                    | 73        |
| Viewing related investigations .....            | 74        |
| Running playbooks in a detection .....          | 74        |
| Entity Panel .....                              | 75        |
| Get a permalink for a device .....              | 77        |
| Device Triage .....                             | 78        |
| Impacted devices .....                          | 78        |

|  |           |
|--|-----------|
| Detection timeline .....                       | 78        |
| Detection rules .....                          | 78        |
| Visualizer .....                               | 79        |
| Filtering the Visualizer .....                 | 80        |
| Nodes .....                                    | 82        |
| Visualizer controls .....                      | 85        |
| Detections Table .....                         | 86        |
| Filtering events .....                         | 86        |
| Statistics .....                               | 88        |
| Manage My Rules .....                          | 89        |
| Creating column profiles .....                 | 90        |
| <b>Investigations .....</b>                    | <b>92</b> |
| Entity Lookup .....                            | 92        |
| Source Device List .....                       | 93        |
| Passive DNS .....                              | 93        |
| Investigate .....                              | 95        |
| Creating investigations .....                  | 96        |
| Viewing investigation details .....            | 97        |
| Adding queries to an investigation .....       | 99        |
| Adding notes to an investigation .....         | 101       |
| Watch an investigation .....                   | 102       |
| Facet Search .....                             | 103       |
| Tag and comment events .....                   | 105       |
| Packet Capture .....                           | 107       |
| Reviewing a task .....                         | 108       |
| Creating a Packet Capture .....                | 108       |
| Terminating and deleting Packet Captures ..... | 109       |
| BPF resources .....                            | 110       |
| PCAP encryption .....                          | 112       |
| Managing encryption keys .....                 | 114       |
| Encryption key settings .....                  | 116       |
| Search Timeline .....                          | 116       |
| Creating queries with Search Timeline .....    | 117       |
| IQL Operators .....                            | 120       |
| Comparison operators .....                     | 121       |
| Logical operators .....                        | 121       |
| Exclude operators .....                        | 122       |
| Pattern operators .....                        | 122       |
| Units .....                                    | 122       |
| Supported units .....                          | 123       |
| Fields with units .....                        | 123       |
| Field reference .....                          | 124       |
| Schema and field references .....              | 124       |
| Event-type expansion .....                     | 124       |
| Field expansion .....                          | 125       |
| Synthetic fields .....                         | 125       |
| Playbooks .....                                | 126       |

|   |            |
|---|------------|
| Running a playbook .....                            | 126        |
| Adding a playbook to an investigation .....         | 127        |
| Running a playbook of event records .....           | 128        |
| Threat intelligence .....                           | 129        |
| Example query: .....                                | 130        |
| Search for intel .....                              | 130        |
| Example search for intel .....                      | 131        |
| <b>Reports .....</b>                                | <b>133</b> |
| <b>Settings .....</b>                               | <b>135</b> |
| Profile settings .....                              | 135        |
| My profile .....                                    | 135        |
| Authentication .....                                | 135        |
| Token .....   | 136        |
| Manage subscriptions .....                          | 136        |
| Manage Annotations .....                            | 137        |
| Sensors .....                                       | 139        |
| Sensor status .....                                 | 141        |
| Account Telemetry .....                             | 143        |
| Sensor settings .....                               | 143        |
| Device view .....                                   | 144        |
| Account management .....                            | 146        |
| Creating users and assigning roles .....            | 147        |
| Settings (Account Management) .....                 | 151        |
| Add or edit a subnet .....                          | 156        |
| Light/Dark Mode .....                               | 157        |
| <b>Sensors deployment .....</b>                     | <b>158</b> |
| Sensor specifications .....                         | 158        |
| Sensor Types .....                                  | 158        |
| Network interfaces for physical sensors .....       | 158        |
| Minimum virtual sensor (ESX) host requirement ..... | 158        |
| Network data sources .....                          | 159        |
| SPAN (mirror) port .....                            | 159        |
| Network TAP .....                                   | 159        |
| Network aggregator .....                            | 160        |
| Complex or combination deployments .....            | 161        |
| Sensor deployment strategy .....                    | 161        |
| Sensor data source configuration .....              | 163        |
| Zscaler ingestion .....                             | 163        |
| Available features .....                            | 164        |
| Deployment services .....                           | 164        |
| Zscaler setup .....                                 | 164        |
| Event comparison .....                              | 171        |
| Sensor provisioning .....                           | 175        |
| Generate a registration code .....                  | 175        |
| Register a sensor .....                             | 176        |

---

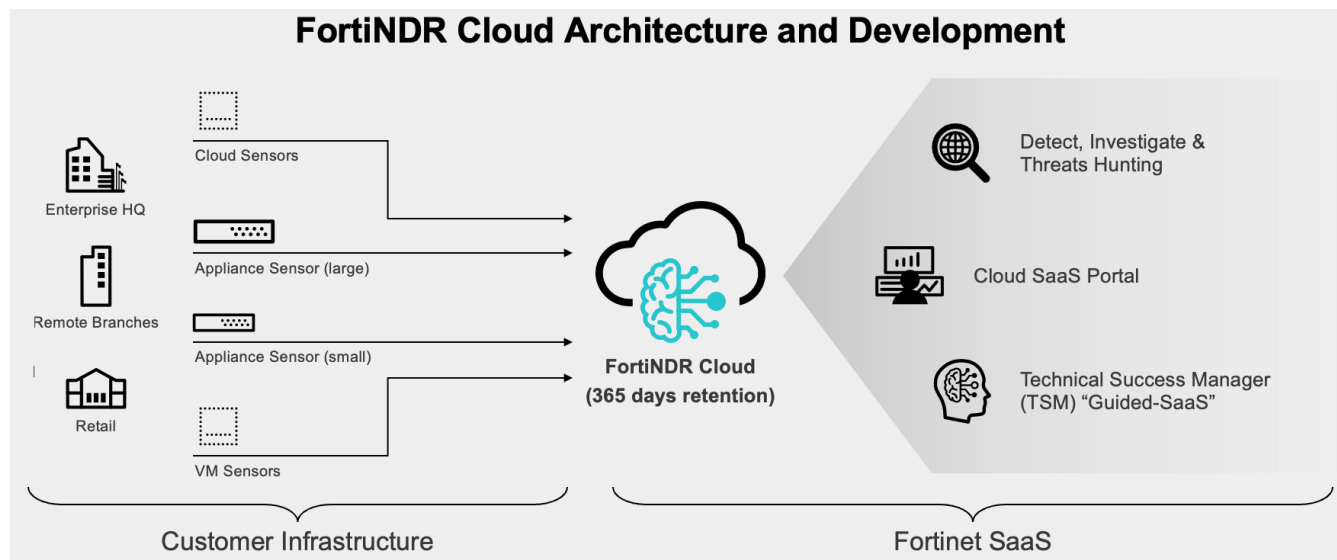
|  |            |
|--|------------|
| <b>FortiNDR Cloud Integrations</b> ..... | <b>178</b> |
| <b>FortiNDR Cloud APIs</b> .....         | <b>179</b> |
| Available APIs .....                     | 179        |
| Metastream .....                         | 179        |

# Change Log

| Date       | Change Description  |
|------------|---|
| 2024-02-29 | Initial release of version <a href="#">2024.2.0</a> .                   |
| 2024-03-04 | Updated <a href="#">Sensor deployment strategy</a> on page 161          |
| 2024-03-13 | Initial release of version <a href="#">2024.2.1</a> .                   |
| 2024-03-15 | Updated <a href="#">Event types and fields</a> on page 11               |
| 2024-03-27 | Initial release of version <a href="#">2024.3.0</a> .                   |
| 2024-03-28 | Updated <a href="#">Creating users and assigning roles</a> on page 147. |
| 2024-4-10  | Initial release of <a href="#">2024.3.1</a> .                           |

# Overview

FortiNDR Cloud is a cloud-native network detection and response solution built for the rapid detection of threat activity, investigation of suspicious behavior, proactive hunting for potential risks, and directing a fast and effective response to active threats.



## Getting started

The following table provides a list of tasks to help you get started with FortiNDR Cloud:

|   |   |
|---|---|
| <b>Enable Multi-Factor Authentication (MFA)</b> | Require all users to enter an MFA token when they log into the FortiNDR Cloud portal.<br>To enable MFA, go to For more information, see <a href="#">Multi-factor authentication</a> .   |
| <b>Configure detection subscriptions</b>        | By default you will receive an email notification for every detection in your account and a daily digest summarizing all of the detections from the past 24 hours.<br>To customize you subscription notifications, go to <i>Settings &gt; Manage Subscriptions</i> . For more information, see <a href="#">Manage subscriptions on page 136</a> . |
| <b>Review the data available to you</b>         | <ul style="list-style-type: none"><li>• <a href="#">Network Entity on page 9</a></li><li>• <a href="#">Network events on page 10</a></li><li>• <a href="#">Enriched object field types on page 13</a></li></ul>   |



**Perform an Entity Lookup**

An *Entity Lookup* is the starting point for an investigation. If you have very little information to work with, because the entity record may contain important contextual information.

For more information, see [Entity Lookup on page 92](#)

**View the Entity Panel**

The *Entity Panel* displays the contextual information collected for an entity from within and outside the network.

For more information, see [Entity Panel on page 75](#).

## Portal navigation

The portal is organized into tabs located in the navigation menu at the top of the portal. Links to the product documentation and *Settings* pages are located in the top-right corner of the page.

**Dashboard**

This is the landing page for the FortiNDR Cloud portal and provides high-level summary information. For more information, see [Dashboard on page 51](#).

**Detections**

This tab shows detections that have fired in your account. For more information, see [Detections on page 59](#).

**Investigations**

This is where you perform queries or run playbooks for forensic analysis and hunting over your network data. For more information, see [Investigations on page 92](#).

**Reports**

Use this tab to run the *FortiNDR Cloud Network Security Posture Report* and the *FortiNDR Cloud Detections Report*. For more information, see [Reports on page 133](#).

**Settings**

This icon located in the top-right provides access to auxiliary pages related to user and account settings and management. For more information, see [Settings on page 135](#).

## Network Entity

An *Entity* is a unique identifier on the network. At this time, IP addresses and domains are supported entities. Entities are extracted from the event data and catalogued in their own data store. Contextual information is then added to the entities when applicable such as:

- First seen / last seen timestamps
- Associated hostnames and usernames from DNS, DHCP, Kerberos, and NTLM events
- WHOIS and Registration information
- VirusTotal intelligence
- Associated software

Entities observed in your account are stored indefinitely. This allows analysts to determine who is interacting with the network and answer questions such as:

- Which / how many of my hosts are interacting with this entity?
- Who is responsible for this entity?
- What other entities are associated with this entity?
- What does everyone else know about this entity?

## Working with entity information

You can perform an *Entity Search* (or Lookup) by simply entering an IP address or domain in the *Search* field at the top navigation menu. An Entity Search is an excellent starting point for an investigation if you have very little information to work with, because the entity record may contain important contextual information. For more information about entity searches, see [Entity Lookup on page 92](#)

The *Entity Panel* displays all of the information collected for an entity from both within and outside of the network. You can access the *Entity Panel* for an entity by left-clicking any entity anywhere in the portal. For more information, see [Entity Panel on page 75](#)

## Network events

FortiNDR Cloud network sensors perform deep packet inspection of all observed network traffic and extract key protocol metadata for processing by the FortiNDR Cloud data pipeline. This metadata is organized into records called *Events*.

### Flow

A *flow* is how FortiNDR Cloud organizes traffic for parsing and tying together events. A flow is a unique session between two hosts. Specifically, a flow is a collection of continuous packets having the same unique five-tuple (source IP, source port, destination IP, destination port, transport protocol) within a short time frame.

Every flow is identified with a unique `flow_id`. Multiple events can be produced from a single flow and are assigned the same `flow_id`.

There three categories of events:

- *Flow events*: The *Flow* event type, contains metadata from the lower layers of the OSI model (IPs, ports, byte counts, transport protocol, etc).
- *Protocol events*: Most event types such as DNS, HTTP, and SSL, contains metadata from the upper layers of the OSI model.
- *Synthetic events*: The *Suricata* and *Software* event types, contains metadata produced by processes that scan or analyze traffic rather than metadata taken directly from network traffic.

Every flow will have exactly one *Flow* event, zero or more protocol events, and zero or more synthetic events. There can only be one *Flow* event because FortiNDR Cloud can summarize all the networking/flow data in one record. There can be zero or more protocol events because the flow could be a raw network socket with no known application, an HTTP connection with numerous HTTP requests over the same connection, an RDP connection over SSL with an X.509 certificate exchanged, or anything else. Similarly, one flow could trigger twelve Suricata signatures just as easily as zero signatures.

Regardless of how many events are produced from a single flow, FortiNDR Cloud assigns them the same unique `flow_id`, which provides a bigger picture surrounding other events in the session.

## Working with events and flows

Running a query will return a list of events. If an event in the list stands out for some reason, you can run a separate query for that event's `flow_id` to see what other events were produced during that session/connection/conversations/flow.

Protocols are parsed regardless of port or service. Events are normalized for time and enriched with Geo-IP information and Threat Intelligence for additional context. Once this processing and enrichment is finished, events are surfaced through the FortiNDR Cloud portal and APIs.

## Event types and fields

This section contains information about the event types available in FortiNDR Cloud, the fields parsed for each event type. Here, as well as an explanation of the fundamental concepts like field types and common fields.

[Event types](#)

[Field types](#)

[Enriched object field types](#)

[Common Fields](#)

[Event fields](#)

## Event types

Each event type contains a set of [common fields](#) (included in all event types) and [event fields](#) (unique to the event type).

The following table shows the event types supported by FortiNDR Cloud:

| Event Type        | Description   |
|-------------------|---|
| <code>flow</code> | An IP-layer network connection                        |
| <code>dns</code>  | A single DNS request and response                     |
| <code>http</code> | A single HTTP request and response                    |
| <code>smtp</code> | An SMTP message                                       |
| <code>ssl</code>  | The creation of an encrypted channel using SSL or TLS |
| <code>x509</code> | An observed x509 record                               |
| <code>rdp</code>  | An attempted Windows RDP connection                   |
| <code>ssh</code>  | An attempted SSH connection                           |

| Event Type               | Description  |
|--------------------------|--|
| <code>ftp</code>         | A single FTP connection, both establishment and data transfer  |
| <code>tunnel</code>      | A single established tunnel  |
| <code>dhcp</code>        | A single DHCP lease  |
| <code>kerberos</code>    | A single Kerberos request from any step of the process   |
| <code>ntlm</code>        | A single NTLM authentication attempt   |
| <code>smb_file</code>    | The transfer of one or more files using SMB  |
| <code>smb_mapping</code> | The mapping of a networked resource using SMB  |
| <code>dce_rpc</code>     | A single DCE/RPC command   |
| <code>pe</code>          | A portable executable (PE) file transferred over a connection  |
| <code>suricata</code>    | A match for a single Suricata signature  |
| <code>software</code>    | An inference of software running on a host based on observed fields from other events                |
| <code>observation</code> | An event generated by the FortiNDR Cloud analytics backend based on a correlation of multiple events |

[Back to top.](#)

## Field types

Most fields are atomic, meaning they cannot be broken down further. However, FortiNDR Cloud fields can also be a structured object, either an object or an array. See [Enriched object field types on page 13](#).

Fields in FortiNDR Cloud can be one of the following types.

| Field Type       | Description   | Example                  |
|------------------|---|--------------------------|
| <i>int</i>       | An integer value (port, bytes, packets, etc.)           | 1                        |
| <i>float</i>     | A decimal value (distance, entropy, etc.)               | 1.0                      |
| <i>Boolean</i>   | true or false   | True                     |
| <i>string</i>    | A sequence of arbitrary characters                      | hello world              |
| <i>timestamp</i> | A RFC3339 timestamp value                               | 2019-01-01T00:00:00.000Z |
| <i>ip</i>        | A single IP address or valid CIDR-notation              | 8.8.8.8, 10.0.1.0/24     |
| <i>object</i>    | An arbitrary JSON structure containing nested subfields | N/A                      |
| <i>array</i>     | An array of values of the same type                     | N/A                      |

[Back to top.](#)

## Enriched object field types

A field that is of type object simply means the field is actually a collection of sub-fields. Some of those sub-fields could also be another collection of sub-fields. Think of an *object* as a JSON block, or a dictionary for the Python users, or a map for the C/C++ users. Sub-fields are then referenced using dot notation, (for example, `dst.geo.country`).

Some object types are very common and are used over and over again, such as an *ip-object*. An *ip-object* refers to a field with the structure shown in the *ip-object* table. These field types are used throughout the different event types, so you should be familiar with them.

The following topics provide a description of each object field type and the sub-fields it contains:

- [IP-Objects on page 13](#)
- [Domain-Objects on page 14](#)
- [Host-Objects on page 14](#)
- [URI-Objects on page 15](#)
- [URL-Objects on page 15](#)
- [File-Objects on page 16](#)
- [Email-Objects on page 16](#)

[Back to top.](#)

## IP-Objects

The following table describes the fields that contain enriched information for an IP address:

| Field                 | Type                   | Description   | Example                 |
|-----------------------|------------------------|---|-------------------------|
| <code>asn</code>      | <i>asn-object</i>      | ASN information for the IP address  | See table below         |
| <code>\$device</code> | <i>synthetic field</i> | Enables querying devices by hostname or MAC address. Note: this field is only available for the <code>src</code> and <code>dst</code> fields. | N/A                     |
| <code>geo</code>      | <i>geo-object</i>      | Geographic information for the IP address   | See table below         |
| <code>internal</code> | <i>Boolean</i>         | Indicates whether the IP address is internal to the network   | <code>true</code>       |
| <code>ip</code>       | <i>ip</i>              | The IP address  | 10.10.10.10             |
| <code>ip_bytes</code> | <i>int</i>             | The number of bytes transmitted by the IP address within the flow (only populated in Flow events)   | 458 Bytes               |
| <code>pkts</code>     | <i>int</i>             | The number of packets transmitted by the IP address within the flow (only populated in Flow events)   | 8                       |
| <code>port</code>     | <i>int</i>             | The port used by the IP address   | 52843                   |
| <code>username</code> | <i>int</i>             | The user name from Zscaler used in device detections (only populated in DNS, Flow, HTTP, and SSL events).                                     | john.smith@fortinet.com |

| Field    | Type       | Description   | Example     |
|----------|------------|---|-------------|
| hostname | <i>int</i> | The host name from Zscaler used in device detections (only populated in DNS, Flow, HTTP, and SSL events). | F09NQJM1ABC |

The `asn` field contains the following subfields.

| Field       | Type          | Description   | Example             |
|-------------|---------------|---|---------------------|
| asn         | <i>int</i>    | The Autonomous System Number  | 16509               |
| asn_<br>org | <i>string</i> | The organization name associated with the ASN (they actually use the ASN) | Amazon.com,<br>Inc. |
| isp         | <i>string</i> | The upstream ISP for the ASN  | Amazon.com          |
| org         | <i>string</i> | The upstream owner of the ASN - may differ from <code>asn_org</code>      | Amazon.com          |

The `geo` field contains the following subfields.

| Field       | Type          | Description                                   | Example              |
|-------------|---------------|---|----------------------|
| city        | <i>string</i> | The city of record                            | Boardman             |
| country     | <i>string</i> | The country of record                         | US                   |
| location    | <i>object</i> | The longitude and latitude of record          | (45.8491, -119.7143) |
| subdivision | <i>string</i> | The segment of the country (states in the US) | OR                   |

[Back to top.](#)

[Back to Enriched object field types.](#)

## Domain-Objects

The following table describes the fields that contain enriched information for a domain:

| Field              | Type          | Description                                | Example                        |
|--------------------|---------------|--|--------------------------------|
| domain             | <i>string</i> | The domain                                 | portal.fortindr.forticloud.com |
| domain_<br>entropy | <i>float</i>  | The computed Shannon entropy of the domain | 3.5                            |

[Back to top.](#)

[Back to Enriched object field types.](#)

## Host-Objects

Host-Objects fields contain enriched information for both IP addresses and domains because the field could be either one. For example an HTTP Host header or a DNS answer.

Host-Objects contain the combined sub-fields in:

- [IP-Objects on page 13](#)
- [Domain-Objects on page 14](#)

[Back to top.](#)

[Back to Enriched object field types.](#)

## URI-Objects

Fields that contain a URI are broken up into its different components.

| Field    | Type                | Description  | Example  |
|----------|---------------------|--|--|
| fragment | <i>string</i>       | The fragment identifier component                  | #  |
| host     | <i>host-object</i>  | The content of the Host header                     | portal.fortindr.forticloud.com   |
| params   | <i>object-array</i> | The HTTP parameters as an array of key-value pairs | N/A  |
| path     | <i>string</i>       | The path of the requested resource                 | search   |
| port     | <i>integer</i>      | The specified port                                 | 443  |
| query    | <i>string</i>       | The full parameter string                          | query=8.8.8.8&sort_dir=desc  |
| scheme   | <i>string</i>       | The specified scheme                               | https  |
| uri      | <i>string</i>       | The full URI                                       | https://portal.fortindr.forticloud.com:443/search?query=8.8.8.8&sort_dir=desc# |

## URL-Objects

Fields that contain both a *host-object* and a *uri-object* are referred to as a *url-object*.

URL-Objects contain the combined sub-fields in:

- [IP-Objects on page 13](#)
- [Domain-Objects on page 14](#)
- [URI-Objects on page 15](#)

[Back to top.](#)

[Back to Enriched object field types.](#)

## File-Objects

File-Objects fields contain enriched information for an observed file.

| Field     | Type          | Description                 | Example  |
|-----------|---------------|-----------------------------|--|
| bytes     | <i>int</i>    | The file's size in bytes    | 145922   |
| md5       | <i>string</i> | The computed MD5 hash       | 92a4d0aeede3ce110b4121342df48496                                 |
| mime_type | <i>string</i> | The fingerprinted MIME-type | application/x-dosexec  |
| name      | <i>string</i> | The observed name           | 2487ff63fb4e79.gif   |
| sha1      | <i>string</i> | The computed SHA1 hash      | e63932430d4028b51fa25dae13d9e0188e9a02a5                         |
| sha256    | <i>string</i> | The computed SHA256 hash    | 227193160a2448dfa8bbbd2cf125afa9cca0d1a718b109a3adae5df8a24cdf6e |

[Back to top.](#)

[Back to Enriched object field types.](#)

## Email-Objects

Email-Objects fields contain an email address broken up into its different components.

| Field  | Type          | Description              | Example        |
|--------|---------------|--------------------------|----------------|
| domain | <i>string</i> | The domain               | gmail.com      |
| email  | <i>string</i> | The entire email address | jdoe@gmail.com |
| name   | <i>string</i> | The name                 | jdoe           |



[Back to top.](#)

[Back to Enriched object field types.](#)

## Common fields

There are a handful of fields that appear in every event type. Some fields are for housekeeping, such as a unique identifier for every event or the sensor that created the event, while others are fundamental to network traffic, such as timestamps and source/destination IP addresses. Each of the following fields are contained in every event with a few exceptions documented in the table below.

| Field        | Type               | Description  | Example                              |
|--------------|--------------------|--|--------------------------------------|
| account      | <i>string</i>      | The name of the account that owns the event  | Training                             |
| customer_id  | <i>string</i>      | The code of the account that owns the event  | chg                                  |
| dst          | <i>ip-object</i>   | The responder to the connection  | 8.8.8.8                              |
| flow_id      | <i>string</i>      | A unique identifier for a flow shared by all events produced from that particular flow | CtjvJR1nIzN4WFSuc7                   |
| geo_distance | <i>float</i>       | The difference between <code>src</code> and <code>dst</code> geo values                | 1410.373826280689                    |
| intel        | <i>intel-array</i> | An array of intel-objects matching entities in the event                               | N/A                                  |
| sensor_id    | <i>string</i>      | The sensor that created the event  | chg1                                 |
| src          | <i>ip-object</i>   | The initiator of the connection  | 10.10.10.10                          |
| timestamp    | <i>timestamp</i>   | The time at which traffic for the event began  | 2019-01-01T00:00:00.000Z             |
| uuid         | <i>string</i>      | A unique identifier for the event  | 1ca116cb-9262-11e9-b5bf-02472fee9a4a |

The `intel` field is an array of values of type *intel-object*. The table below lists the sub-fields contained within the `intel` field.

| Field          | Type           | Description                                       | Example       |
|----------------|----------------|---|---------------|
| confidence     | <i>string</i>  | The overall confidence rating of the intel source | high          |
| feed           | <i>string</i>  | The name of the intel source                      | Sinkholes     |
| indicator      | <i>string</i>  | The matched entity                                | 131.253.18.12 |
| indicator_type | <i>string</i>  | The entity type                                   | ip_address    |
| is_            | <i>Boolean</i> | Indicates whether the                             | false         |

| Field     | Type             | Description  | Example   |
|-----------|------------------|--|---|
| malicious |                  | indicator is believed to be malicious                      |   |
| meta      | <i>string</i>    | A JSON string of all metadata provided by the intel source | {"description": "Observed C2 Activity", "references": ["Fortinet FortiGuard Labs"]} |
| severity  | <i>string</i>    | The overall severity rating of the intel source            | high  |
| timestamp | <i>timestamp</i> | The creation time of the intel record                      | 2019-01-01T00:00:00.000Z  |

## Exceptions to common fields

1. The `software` event type does not have `src` and `dst` fields because it is not extracted from raw network traffic. Instead, the record is inferred based on the contents of one or more fields.
2. The `suricata` event type does not have a `flow_id` field because it is generated by a completely different process than the other event types. You must match `suricata` events to their associated flows using the IP address and ports of the event.

See also [Common fields on page 17](#).

[Back to top](#).

## Event fields

The following topics describe the fields unique to each event type.

- [DCE RPC fields on page 36](#)
- [DHCP fields on page 32](#)
- [DNS fields on page 20](#)
- [Flow fields on page 19](#)
- [FTP fields on page 31](#)
- [HTTP fields on page 21](#)
- [Kerberos fields on page 33](#)
- [Notice Fields on page 40](#)
- [NTLM fields on page 34](#)
- [Observation fields on page 39](#)
- [PE fields on page 36](#)
- [RDP fields on page 27](#)
- [SMB file fields on page 35](#)
- [SMB mapping fields on page 35](#)
- [SMTP fields on page 25](#)
- [Software fields on page 38](#)
- [SSH fields on page 30](#)
- [SSL fields on page 28](#)

- [Suricata fields on page 37](#)
- [Tunnel fields on page 32](#)
- [x509 fields on page 29](#)

[Back to top.](#)

## Flow fields

A `flow` event is created whenever packets with a unique combination of `src.ip`, `src.port`, `dst.ip`, `dst.port`, and `proto` are observed within a sufficient time frame.

The following table shows fields unique to the `flow` event type:

| Field                       | Type          | Description   | Example                |
|-----------------------------|---------------|---|------------------------|
| <code>duration</code>       | <i>float</i>  | The number of seconds the flow lasted   | <code>7s</code>        |
| <code>flow_state</code>     | <i>string</i> | Indicates how the connection started and ended, hover over a value to get an explanation of it      | <code>SF</code>        |
| <code>proto</code>          | <i>string</i> | The transport layer protocol used   | <code>tcp</code>       |
| <code>service</code>        | <i>string</i> | The application(s) observed in the flow, if any   | <code>http</code>      |
| <code>total_ip_bytes</code> | <i>int</i>    | The total combined bytes transmitted over the connection  | <code>927 bytes</code> |
| <code>total_pkts</code>     | <i>int</i>    | The total combined packets transmitted over the connection  | <code>11</code>        |
| <code>upload_percent</code> | <i>int</i>    | The percentage of bytes transmitted by the <code>src</code> for the flow ( <code>56% == 56</code> ) | <code>56%</code>       |

[Back to top.](#)

[Back to Event Fields.](#)

## flow\_state

The following table lists the different `flow_state` values and a brief description for each:

| flow_state       | Description  |
|------------------|--|
| <code>S0</code>  | Connection attempt seen, no reply.   |
| <code>S1</code>  | Connection established, not terminated.  |
| <code>SF</code>  | Normal establishment and termination.  |
| <code>REJ</code> | Connection attempt rejected.   |
| <code>S2</code>  | Connection established and close attempt by originator seen (but no reply from responder). |
| <code>S3</code>  | Connection established and close attempt by responder seen (but no reply from              |

| flow_state | Description  |
|------------|--|
|            | originator).   |
| RSTO       | Connection established, originator aborted (sent a RST).   |
| RSTR       | Responder sent a RST.  |
| RSTOS0     | Originator sent a SYN followed by a RST, we never saw a SYN-ACK from the responder.  |
| RSTRH      | Responder sent a SYN ACK followed by a RST, we never saw a SYN from the (purported) originator.                            |
| SH         | Originator sent a SYN followed by a FIN, we never saw a SYN ACK from the responder (hence the connection was "half" open). |
| SHR        | Responder sent a SYN ACK followed by a FIN, we never saw a SYN from the originator.  |
| OTH        | No SYN seen, just midstream traffic (a "partial connection" that was not later closed).                                    |

[Back to top.](#)

[Back to Event Fields.](#)

## DNS fields

A `dns` event is created when a client submits a DNS request to a server, and includes data from both the request and the response (if a response was observed).

The following table shows fields unique to the `dns` event type:

| Field                   | Type                     | Description  | Example                      |
|-------------------------|--------------------------|--|------------------------------|
| <code>answers</code>    | <i>host-object-array</i> | The answers returned by the DNS server for the query   | [103.2.116.79, 103.2.116.83] |
| <code>proto</code>      | <i>string</i>            | The transport layer protocol used                      | udp                          |
| <code>qtype</code>      | <i>int</i>               | The numeric code of the query type                     | 1                            |
| <code>qtype_name</code> | <i>string</i>            | The string name of the query type                      | A                            |
| <code>query</code>      | <i>domain-object</i>     | The domain being queried                               | www.google.com               |
| <code>rcode</code>      | <i>int</i>               | The numeric code of the result                         | 0                            |
| <code>rcode_name</code> | <i>int</i>               | The string name of the result                          | NOERROR                      |
| <code>rejected</code>   | <i>Boolean</i>           | Indicates whether the query was rejected by the server | false                        |
| <code>ttls</code>       | <i>int-array</i>         | An array of TTL values, one per result                 | [299, 299]                   |

[Back to top.](#)

[Back to Event Fields.](#)

## HTTP fields

An `http` event is created when a client submits an HTTP request to a server, and includes data from both the request and response (if the response was observed).

The following table shows fields unique to the `http` event type:

| Field                              | Type                     | Description                                  | Example   |
|------------------------------------|--------------------------|--|---|
| <code>files</code>                 | <i>file-object-array</i> | Files downloaded over the HTTP connection    | N/A   |
| <code>headers.accept</code>        | <i>string-array</i>      | The content of the Accept header             | [image/webp, image/apng, image/*, */*;q=0.8]                                    |
| <code>headers.content_md5</code>   | <i>string</i>            | The computed MD5 hash of the headers content | d41d8cd98f00b204e9800998ecf8427e  |
| <code>headers.content_type</code>  | <i>string-array</i>      | The contents of the Content Type header      | [text/xml; charset="utf-8"]   |
| <code>headers.cookie_length</code> | <i>int</i>               | The length of the cookie in bytes            | 194   |
| <code>headers.location</code>      | <i>url-object</i>        | The content of the Location header           | http://amupdated13.microsoft.com/server/amupdate/metadata/UniversalManifest.cab |
| <code>headers.origin</code>        | <i>url-object</i>        | The content of the                           | http://go.com   |

| Field                      | Type            | Description  | Example   |
|----------------------------|-----------------|--|---|
|                            |                 | Origin header  |   |
| headers.proxied_ip_clients | ip-object-array | The sequence of IPs the HTTP connection is proxied through | [172.16.0.1, 172.16.0.2]                          |
| headers.refresh.refresh    | string          | The full content of the Refresh header                     | 1;URL=http://travelingtravelerhome.wordpress.com/ |
| headers.refresh.timeout    | int             | The timeout period in seconds                              | 1   |
| headers.refresh.uri        | uri-object      | The URI of the Refresh header                              | http://travelingtravelerhome.wordpress.com/       |
| headers.server             | string          | The web server software                                    | Microsoft-IIS/6.0                                 |
| headers.x_powered_by       | string          | The application software running on the server             | ASP.NET   |
| host                       | host-object     | The content Host header                                    | www.google.com                                    |
| info_msg                   | string          | The message returned with a                                | Continue  |

| Field         | Type                | Description  | Example   |
|---------------|---------------------|--|---|
|               |                     | 100-level response code  |   |
| method        | <i>string</i>       | The HTTP method selected   | GET   |
| proxied       | <i>string-array</i> | A list of proxy steps  | PROXY-CONNECTION -> Keep-Alive  |
| referrer      | <i>url-object</i>   | The content of the Referrer header   | http://au.search.yahoo.com/search?p=planetside.co.uk&fr=sfp&fr2=sb-top-search |
| request_len   | <i>int</i>          | The length in bytes of the request   | 0   |
| request_mime  | <i>string</i>       | The fingerprinted MIME-type(s) of the request content ( <b>deprecated</b> )        | text/plain  |
| request_mimes | <i>string-array</i> | The fingerprinted MIME-type(s) of the request content, use instead of request_mime | text/plain  |

| Field          | Type                | Description   | Example                             |
|----------------|---------------------|---|-------------------------------------|
| response_len   | <i>int</i>          | 24  | The length in bytes of the response |
| response_mime  | <i>string</i>       | The fingerprinted MIME-type of the response content ( <b>deprecated</b> )         | text/html                           |
| response_mimes | <i>string-array</i> | The fingerprinted MIME-type of the response content, use instead of response_mime | text/html                           |
| status_code    | <i>int</i>          | The numeric code of the server's response   | 200                                 |
| status_msg     | <i>string</i>       | The string name of the server's response  | OK                                  |
| trans_depth    | <i>int</i>          | The depth of redirects  | 4                                   |
| uri            | <i>uri-object</i>   | The full URI of the request   | /index.php                          |



| Field      | Type          | Description                               | Example  |
|------------|---------------|---|--|
| user_agent | <i>string</i> | The content of the UserAgent header       | Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko |
| username   | <i>string</i> | The username used with Basic Auth, if any | dave   |

[Back to top.](#)

[Back to Event Fields.](#)

## SMTP fields

An `smtp` event is created when a client transmits an SMTP message to a server.

The following table shows fields unique to the `smtp` event type:

| Field          | Type                     | Description                                   | Example   |
|----------------|--------------------------|---|---|
| date           | <i>string</i>            | The content of the Date header                | Thu, 12 Jul 2015 17:59:01 -0400 (EDT)   |
| files          | <i>file-object-array</i> | An array of the files attached to the email   | N/A   |
| first_received | <i>string</i>            | The full content of the first Received header | from JIM@GMAIL.COM ([198.51.100.1]) by SALLY@GMAIL.COM ([101.9.210.120]) with mapi id 14.01.1039.013; Thu, 12 Jul 2015 18:09:44 -0500 |
| from           | <i>email-object</i>      | The content of the From header                | jdoe@gmail.com  |
| helo           | <i>host-object</i>       | The argument supplied to the HELO command     | client.example.com  |
| in_reply_to    | <i>string</i>            | The Message-ID in the In-                     | <b8bba2baae4c2a08fdff4e223458577d@gmail.com>  |

| Field           | Type                   | Description  | Example   |
|-----------------|------------------------|--|---|
|                 |                        | Reply-To header  |   |
| is_webmail      | <i>Boolean</i>         | Indicates whether the message was sent through a webmail interface | true  |
| last_reply      | <i>string</i>          | The last message the server sent to the client                     | 250 Message accepted for delivery   |
| mailfrom        | <i>string</i>          | The argument supplied to the MAIL FROM command                     | support@acme.corp   |
| msg_id          | <i>string</i>          | The Message-ID of the message                                      | <b8bba2baae4c2a08fdff4e223458577d@gmail.com>  |
| path            | <i>ip-object-array</i> | The message transmission path extracted from the Received headers  | [192.161.0.200, 204.148.78.113]   |
| rcptto          | <i>string</i>          | The argument supplied to the RCPT TO command                       | jdoe@gmail.com  |
| reply_to        | <i>email-object</i>    | The content of the Reply-To header                                 | jdoe@gmail.com  |
| second_received | <i>string</i>          | The content of the second Received header                          | from JIM@GMAIL.COM ([198.51.100.1]) by SALLY@GMAIL.COM ([101.9.210.120]) with mapi id 14.01.1039.013; Thu, 12 Jul 2015 18:09:44 -0500 |
| subject         | <i>string</i>          | The content of the Subject header                                  | Click this link!  |
| tls             | <i>Boolean</i>         | Indicates whether the  | true  |

| Field            | Type                      | Description   | Example  |
|------------------|---------------------------|---|--|
|                  |                           | connection switched to using TLS  |  |
| to               | <i>email-object-array</i> | The content of the To header  | [jdoe@gmail.com, kdoe@gmail.com]                       |
| trans_depth      | <i>int</i>                | The depth of this message transaction where multiple messages were transferred in a single connection | 1  |
| urls             | <i>string-array</i>       | A list of URLs extracted from the message   | [http://malware.pwn//root.psl, https://www.google.com] |
| user_agent       | <i>string</i>             | The content of the client's User-Agent header   | SquirrelMail/1.4.22                                    |
| x_originating_ip | <i>ip-object</i>          | The content of the X-Originating-IP header  | 8.8.8.8  |

[Back to top.](#)

[Back to Event Fields.](#)

## RDP fields

An `rdp` event is created when a client attempts to connect to a server using RDP.



Authentication cannot always be determined as the necessary data may be encapsulated within an encrypted tunnel. Therefore, the `result` field may contain a "best-guess" based on available data.

The following table shows fields unique to the `rdp` event type:

| Field      | Type           | Description   | Example |
|------------|----------------|---|---------|
| cert_count | <i>int</i>     | The number of certificates seen                               | 0       |
| cert_      | <i>Boolean</i> | Indicates if the provided certificate or certificate chain is | True    |

| Field                 | Type          | Description   | Example                         |
|-----------------------|---------------|---|---------------------------------|
| permanent             |               | permanent   |                                 |
| cert_type             | <i>string</i> | The type of certificate used if the connection is encrypted with native RDP encryption  | RSA                             |
| client_build          | <i>string</i> | The client RDP version  | RDP 5.1                         |
| client_dig_product_id | <i>string</i> | The client product ID   | 715e03e8-6eef-4c53-b022-rbcd967 |
| client_name           | <i>string</i> | The client hostname   | bob-PC                          |
| cookie                | <i>string</i> | The truncated account name used by the client   | bob                             |
| desktop_height        | <i>int</i>    | The client desktop height   | 1080                            |
| desktop_width         | <i>int</i>    | The client desktop width  | 1920                            |
| encryption_level      | <i>string</i> | The encryption level used   | Client compatible               |
| encryption_method     | <i>string</i> | The encryption method used  | 128bit                          |
| keyboard_layout       | <i>string</i> | The client keyboard layout (language)   | English - United States         |
| requested_color_depth | <i>string</i> | The color depth requested by the client in the high_color_depth field   | 32bit                           |
| result                | <i>string</i> | The result for the connection, derived from a mix of RDP negotiation failure messages and GCC server create response messages | Succeed                         |
| security_protocol     | <i>string</i> | Security protocol chosen by the server  | RDP                             |

[Back to top.](#)

[Back to Event Fields.](#)

## SSL fields

An `ssl` event is created when a client attempts to establish an encrypted channel with a server using SSL/TLS.

The following table shows fields unique to the `ssl` event type:

| Field  | Type          | Description                             | Example                                 |
|--------|---------------|---|---|
| cipher | <i>string</i> | The cipher suite selected by the server | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 |

| Field                  | Type                 | Description  | Example   |
|------------------------|----------------------|--|---|
| client_issuer          | <i>string</i>        | The Issuer field of the client's certificate                               | CN=Google Internet Authority G2,O=Google Inc,C=US |
| client_subject         | <i>string</i>        | The Subject field of the client's certificate                              | CN=*.google.com,O=Google Inc                      |
| issuer                 | <i>string</i>        | The Issuer field of the server's certificate                               | CN=Google Internet Authority G2,O=Google Inc,C=US |
| ja3                    | <i>string</i>        | The computed JA3 hash for the client                                       | 4d7a28d6f2263ed61de88ca66eb011e3                  |
| ja3s                   | <i>string</i>        | The computed JA3 hash of the server  | 4d7a28d6f2263ed61de88ca66eb011e3                  |
| server_name            | <i>string</i>        | The Server Name Indication set by the client ( <i>deprecated</i> )         | www.google.com                                    |
| server_name_indication | <i>domain-object</i> | The enriched Server Name Indication set by the client                      | www.google.com                                    |
| session_id             | <i>string</i>        | The ID used for session resumption ( <i>deprecated</i> )                   | N/A   |
| subject                | <i>string</i>        | The Subject field of the server's certificate                              | CN=*.google.com,O=Google Inc                      |
| validation_status      | <i>string</i>        | Result of certificate validation for this connection ( <i>deprecated</i> ) | Success   |
| version                | <i>string</i>        | The SSL/TLS version being used (period omitted)                            | TLSv10  |

[Back to top.](#)

[Back to Event Fields.](#)

## x509 fields

An x509 event is created when an X.509 certificate is observed over a connection, such as establishing an SSL connection or encrypting an RDP session.

The following table shows fields unique to the x509 event type:

| Field              | Type           | Description                          | Example |
|--------------------|----------------|--------------------------------------|---------|
| ca_constraints     | <i>Boolean</i> | Indicates whether the CA flag is set | False   |
| ca_constraints_len | <i>int</i>     | The maximum path length              | 10      |

| Field       | Type               | Description                                   | Example   |
|-------------|--------------------|---|---|
| cert_id     | <i>string</i>      | The file ID of the certificate                | FNbDqq2ZxjNk10D7ie                              |
| issuer      | <i>string</i>      | The content of the Issuer field               | O=Internet Widgits Pty Ltd, ST=Some-State, C=AU |
| key_len     | <i>int</i>         | The length of the key                         | 2048  |
| key_type    | <i>string</i>      | The type of key used                          | rsa   |
| san_dns     | <i>host-array</i>  | The list of DNS entries in the SAN            | [*.outlook.com, *.office365.com]                |
| san_email   | <i>email-array</i> | The list of email entries in the SAN          | [dave@email.corp]                               |
| san_ip      | <i>ip-array</i>    | The list of IP entries in the SAN             | [169.254.1.1]                                   |
| san_uri     | <i>uri-array</i>   | The list of URI entries in the SAN            | [https://169.254.1.1]                           |
| serial      | <i>string</i>      | The serial number of the certificate          | E3BD4F4F884EADDA                                |
| subject     | <i>string</i>      | The content of the Subject field              | O=Internet Widgits Pty Ltd, ST=Some-State, C=AU |
| valid_end   | <i>timestamp</i>   | The time before the certificate became valid  | 2018-01-11T14:35:34.000Z                        |
| valid_start | <i>timestamp</i>   | The time once the certificate becomes invalid | 2018-01-11T14:35:34.000Z                        |
| version     | <i>string</i>      | The X.509 version                             | 3   |

[Back to top.](#)

[Back to Event Fields.](#)

## SSH fields

An `ssh` event is created when a client attempts to connect to a server using SSH.



Authentication cannot be accurately determined because the necessary data is encapsulated within the encrypted tunnel. Therefore, the `auth_success` field contains a "best-guess" based on available data.

The following table shows fields unique to the `ssh` event type:

| Field        | Type           | Description                        | Example    |
|--------------|----------------|------------------------------------|------------|
| auth_success | <i>Boolean</i> | The inferred authentication result | True       |
| cipher_alg   | <i>string</i>  | The encryption algorithm used      | aes128-ctr |

| Field           | Type          | Description  | Example   |
|-----------------|---------------|--|---|
| client          | <i>string</i> | The client version string  | SSH-2.0-OpenSSH_7.6                             |
| compression_alg | <i>string</i> | The compression algorithm used   | none  |
| direction       | <i>string</i> | The direction of the connection, Outbound if the client was a local host logging into an external host and Inbound in the opposite situation | Inbound   |
| host_key        | <i>string</i> | The server fingerprint   | a1:a2:79:80:6d:b1:77:82:d8:6c:aa:ee:25:19:23:42 |
| host_key_alg    | <i>string</i> | The server's key algorithm.  | ssh-rsa   |
| kex_alg         | <i>string</i> | The key exchange algorithm used  | ecdh-sha2-nistp256                              |
| mac_alg         | <i>string</i> | The signing (MAC) algorithm used   | hmac-sha1                                       |
| server          | <i>string</i> | The server version string  | SSH-2.0-OpenSSH_7.4                             |
| ssh_version     | <i>int</i>    | The SSH major version (1 or 2)   | 2   |

[Back to top.](#)

[Back to Event Fields.](#)

## FTP fields

An `ftp` event is created when a client connects to a server using FTP, and includes both the command and data channels.

The following table shows fields unique to the `ftp` event type:

| Field            | Type             | Description                 | Example  |
|------------------|------------------|-----------------------------|----------|
| data_channel.dst | <i>ip-object</i> | The destination of the data | 10.0.0.2 |

| Field                     | Type              | Description  | Example                                 |
|---------------------------|-------------------|--|---|
|                           |                   | channel  |   |
| data_channel.geo_distance | <i>float</i>      | The distance (in miles) between the IP addresses of the data channel | 5077.89                                 |
| data_channel.passive      | <i>Boolean</i>    | Indicates whether the session is in passive mode                     | True                                    |
| data_channel.src          | <i>ip-object</i>  | The source of the data channel                                       | 10.0.0.10                               |
| files                     | <i>file-array</i> | Files transferred over the session                                   | N/A                                     |
| ftp_arg                   | <i>string</i>     | The full argument string supplied to the command                     | ftp://10.0.0.2/secrets.zip              |
| ftp_command               | <i>string</i>     | The client command   | RETR                                    |
| reply_code                | <i>int</i>        | The server response code to the command                              | 227                                     |
| reply_msg                 | <i>string</i>     | The server response string to the command                            | Entering Passive Mode (10,0,0,2,197,36) |
| username                  | <i>string</i>     | The username used to establish the connection                        | Admin101                                |

[Back to top.](#)

[Back to Event Fields.](#)

## Tunnel fields

A `tunnel` event is created when a tunnel is established between a client and a server.

The following table shows fields unique to the `tunnel` event type:

| Field         | Type          | Description                                      | Example          |
|---------------|---------------|--|------------------|
| tunnel_action | <i>string</i> | The action taken on the tunnel                   | Tunnel::DISCOVER |
| tunnel_type   | <i>string</i> | The protocol/application running over the tunnel | Tunnel::HTTP     |

[Back to top.](#)

[Back to Event Fields.](#)

## DHCP fields

A `dhcp` event is created when a client requests a DHCP lease or when a lease is acknowledged.



The following table shows fields unique to the `dhcp` event type:

| Field                       | Type             | Description   | Example                  |
|-----------------------------|------------------|---|--------------------------|
| <code>assignment</code>     | <i>ip-object</i> | The IP assigned to the client                                   | 10.0.0.10                |
| <code>dhcp_msg_type</code>  | <i>string</i>    | Shows whether a lease is being requested or acknowledged        | Request                  |
| <code>hostname</code>       | <i>string</i>    | The client hostname   | bob-pc                   |
| <code>lease_duration</code> | <i>float</i>     | Number of seconds that the lease is valid                       | 1800                     |
| <code>lease_end</code>      | <i>timestamp</i> | The time at which the lease expires                             | 2019-06-24T07:31:35.012Z |
| <code>mac</code>            | <i>string</i>    | The client MAC address  | 00:30:67:f1:2d:63        |
| <code>trans_id</code>       | <i>int</i>       | The transaction ID, ties together requests and acknowledgments. | 1191705957               |

[Back to top.](#)

[Back to Event Fields.](#)

## Kerberos fields

A `kerberos` event is created when a client uses Kerberos to authenticate.

The following table shows fields unique to the `kerberos` event type:

| Field                            | Type           | Description   | Example                                       |
|----------------------------------|----------------|---|---|
| <code>cipher</code>              | <i>string</i>  | The cipher suite used to encrypt the ticket   | aes256-cts-hmac-sha1-96                       |
| <code>client</code>              | <i>string</i>  | The client that requested the ticket; machine accounts have a \$ at the end of their name but user accounts do not. | jane.doe/ACME.CORP, financewks008\$/ACME.CORP |
| <code>client_cert_fuid</code>    | <i>string</i>  | Client certificate file unique ID   | Xbtku3TdsfdsdfasdfA8VNsk                      |
| <code>client_cert_subject</code> | <i>string</i>  | Client certificate Subject field  | CN=C865433                                    |
| <code>error_msg</code>           | <i>string</i>  | The error message returned for failed requests  | KDC_ERR_CLIENT_NAME_MISMATCH                  |
| <code>forwardable</code>         | <i>Boolean</i> | Indicates whether the ticket's forwardable flag is set  | True  |
| <code>renewable</code>           | <i>Boolean</i> | Indicates whether the ticket's renewable flag is set  | True  |

| Field               | Type             | Description   | Example                  |
|---------------------|------------------|---|--------------------------|
| request_type        | <i>string</i>    | The type of ticket requested, either a ticket-granting ticket from the authentication server (AS) or a service ticket from the ticket-granting server (TGS) | AS, TGS                  |
| server_cert_fuid    | <i>string</i>    | Server certificate file unique ID   | FvAdJGsjeXuhSvE9m        |
| server_cert_subject | <i>string</i>    | Server certificate Subject field  | CN=dc09.google.com       |
| service             | <i>string</i>    | The service for which a ticket is being requested   | krbtgt/ACME.CORP         |
| success             | <i>Boolean</i>   | Indicates whether the request was successful  | True                     |
| ticket_duration     | <i>float</i>     | The ticket duration in seconds  | 86400                    |
| ticket_from         | <i>timestamp</i> | Time the ticket is good from  | 2015-09-13T02:48:05.000Z |
| ticket_till         | <i>timestamp</i> | Time the ticket is good until   | 2037-09-13T02:48:05.000Z |

[Back to top.](#)

[Back to Event Fields.](#)

## NTLM fields

An `ntlm` event is created when a client uses NTLM to authenticate to a server.

The following table shows fields unique to the `ntlm` event type:

| Field       | Type           | Description  | Example       |
|-------------|----------------|--|---------------|
| auth_domain | <i>string</i>  | The domain used to authenticate the client         | ACME          |
| hostname    | <i>string</i>  | The client hostname used                           | FINANCEWKS008 |
| ntlm_status | <i>string</i>  | String indicating the result of the authentication | SUCCESS       |
| success     | <i>Boolean</i> | Indicates whether the authentication succeeded     | True          |
| username    | <i>string</i>  | The client username used                           | sqlservice    |

[Back to top.](#)

[Back to Event Fields.](#)

## SMB file fields

An `smb_file` event is created when a file is transferred over the network through the use of SMB. This event type includes extra fields related MACB timestamps and file paths in addition to the *file-object* fields because SMB includes file metadata during the transfer.

The following table shows fields unique to the `smb_file` event type:

| Field                                 | Type              | Description  | Example  |
|---------------------------------------|-------------------|--|--|
| <code>files</code>                    | <i>file-array</i> | Files transferred over the SMB connection                                  | N/A  |
| <code>files.accessed_timestamp</code> | <i>timestamp</i>  | The last time the file was accessed  | 2018-04-08T22:48:07.958Z                               |
| <code>files.changed_timestamp</code>  | <i>timestamp</i>  | The last time the file's metadata changed                                  | 2018-04-08T22:48:07.958Z                               |
| <code>files.created_timestamp</code>  | <i>timestamp</i>  | The time the file was created  | 2018-04-08T22:48:07.958Z                               |
| <code>files.modified_timestamp</code> | <i>timestamp</i>  | The last time the file's content changed                                   | 2018-04-08T22:48:07.958Z                               |
| <code>files.name</code>               | <i>string</i>     | The post-transfer name of the file (can be renamed before writing to disk) | <code>secrets.zip</code>                               |
| <code>files.previous_name</code>      | <i>string</i>     | The pre-transfer name of the file  | <code>exfil.zip</code>                                 |
| <code>files.smb_path.path</code>      | <i>string</i>     | The full network path to the target share                                  | <code>\\DYNACCOUNTIC-DC.dynaccountic.com\sysvol</code> |
| <code>files.smb_path.share</code>     | <i>string</i>     | The target network share   | <code>sysvol</code>                                    |
| <code>files.smb_path.system</code>    | <i>string</i>     | The target host  | <code>DYNACCOUNTIC-DC.dynaccountic.com</code>          |
| <code>smb_action</code>               | <i>string</i>     | The action taken on the files  | <code>SMB::FILE_OPEN</code>                            |

[Back to top.](#)

[Back to Event Fields.](#)

## SMB mapping fields

An `smb_mapping` event is created when a client attempts to interact with a network share via SMB. This includes both disk and pipe shares.

The following table shows fields unique to the `smb_mapping` event type:

| Field              | Type          | Description   | Example                                   |
|--------------------|---------------|---|---|
| native_file_system | <i>string</i> | The file system type on the target host (for Disk shares) | NTFS                                      |
| share_type         | <i>string</i> | The type of share established                             | DISK                                      |
| smb_path.path      | <i>string</i> | The full network path to the target share                 | \\DYNACCOUNTIC-DC.dynaccountic.com\sysvol |
| smb_path.share     | <i>string</i> | The target network share                                  | sysvol                                    |
| smb_path.system    | <i>string</i> | The target host   | DYNACCOUNTIC-DC.dynaccountic.com          |
| smb_service        | <i>string</i> | The service used to establish a connection to the share   | IPC                                       |

[Back to top.](#)

[Back to Event Fields.](#)

## DCE RPC fields

A `dce_rpc` event is created when one host executes a DCE/RPC command against another host.

The following table shows fields unique to the `dce_rpc` event type:

| Field             | Type          | Description  | Example        |
|-------------------|---------------|--|----------------|
| dce_rpc_endpoint  | <i>string</i> | The remote service targeted by the command                         | samr           |
| dce_rpc_operation | <i>string</i> | The command submitted to the remote service                        | SamrOpenDomain |
| named_pipe        | <i>string</i> | The name of the target pipe (or the destination port if not named) | \pipe\lsass    |
| round_trip_time   | <i>float</i>  | The time in seconds between command execution and results returned | 0.01           |

[Back to top.](#)

[Back to Event Fields.](#)

## PE fields

A `pe` event is created when a portable executable (PE) file or object is transferred over a connection.

The following table shows fields unique to the `pe` event type:

| Field    | Type             | Description                              | Example  |
|----------|------------------|--|----------|
| compile_ | <i>timestamp</i> | The compile timestamp extracted from the | 2015-11- |

| Field               | Type                | Description   | Example                       |
|---------------------|---------------------|---|-------------------------------|
| timestamp           |                     | file  | 12T10:23:51.000Z              |
| file                | <i>file-object</i>  | The enriched file properties (hashes, size, MIME-type)        | N/A                           |
| has_cert_table      | <i>Boolean</i>      | Indicates whether the file has an attribute certificate table | True                          |
| has_debug_data      | <i>Boolean</i>      | Indicates whether the file has a debug table                  | True                          |
| has_export_table    | <i>Boolean</i>      | Indicates whether the file has an export table                | True                          |
| has_import_table    | <i>Boolean</i>      | Indicates whether the file has an import table                | True                          |
| id                  | <i>string</i>       | An internal unique identifier for the file                    | FrkSk6Y0mqKGxMBF6             |
| is64_bit            | <i>Boolean</i>      | Indicates whether the file is 64-bit                          | True                          |
| is_exe              | <i>Boolean</i>      | Indicates whether the file is executable or just an object    | True                          |
| machine             | <i>string</i>       | The architecture the file was compiled for                    | I386                          |
| os                  | <i>string</i>       | The OS the file was compiled for                              | Windows XP                    |
| section_names       | <i>string-array</i> | An array of section names extracted from the file             | [.text, .rdata, .data, .rsrc] |
| subsystem           | <i>string</i>       | The subsystem the file was compiled for                       | WINDOWS_GUI                   |
| uses_aslr           | <i>Boolean</i>      | Indicates whether the file supports ASLR                      | True                          |
| uses_code_integrity | <i>Boolean</i>      | Indicates whether the file enforces code integrity checks     | True                          |
| uses_dep            | <i>Boolean</i>      | Indicates whether the file supports DEP                       | True                          |
| uses_seh            | <i>Boolean</i>      | Indicates whether the file uses SEH                           | True                          |

[Back to top.](#)

[Back to Event Fields.](#)

## Suricata fields

A `suricata` event is created when a Suricata signature fires on a sensor. Signatures from the ET Open ruleset are included by default on all sensors.



Suricata runs independently from the metadata extraction process, and thus is not tied to flow events with a `flow_id` even though both a `suricata` and `flow` event will exist for the traffic. Additionally, directionality is not maintained by Suricata, so the `src.ip` and `dst.ip` fields for a `suricata` event may be reversed from the related `flow`.

The following table shows fields unique to the `suricata` event type:

| Field                     | Type              | Description   | Example                              |
|---------------------------|-------------------|---|--------------------------------------|
| <code>payload</code>      | <i>byte-array</i> | The raw payload from the traffic that matched the signature | N/A                                  |
| <code>proto</code>        | <i>string</i>     | The transport layer protocol used                           | <code>tcp</code>                     |
| <code>sig_category</code> | <i>string</i>     | The signature's category                                    | A Network Trojan was Detected        |
| <code>sig_id</code>       | <i>int</i>        | The signature's ID  | 2024290                              |
| <code>sig_name</code>     | <i>string</i>     | The signature's name  | ET_TROJAN_Jaff Ransomware Checkin M1 |
| <code>sig_rev</code>      | <i>float</i>      | The signature's revision number                             | 2                                    |
| <code>sig_severity</code> | <i>int</i>        | The signature's severity rating (1 = high, 3 = low)         | 1                                    |

[Back to top.](#)

[Back to Event Fields.](#)

## Software fields

A `software` event is created when sufficient data is observed to fingerprint software running on a host. Such data could include a User-Agent string or a client version string.



Software events do not have a `src` or `dst` column like all other event types because they only refer to behavior observed from one host and not the underlying connection.

The following table shows fields unique to the `software` event type.

| Field                                    | Type             | Description                                   | Example                    |
|--|------------------|---|----------------------------|
| <code>host</code>                        | <i>ip-object</i> | The host from which the software was observed | <code>10.0.0.10</code>     |
| <code>software_name</code>               | <i>string</i>    | The name of the observed software             | <code>Wget</code>          |
| <code>software_type</code>               | <i>string</i>    | The category of the observed software         | <code>HTTP::BROWSER</code> |
| <code>software_version.additional</code> | <i>string</i>    | Arbitrary notes about the software            | <code>linux-gnu</code>     |
| <code>software_version.major</code>      | <i>int</i>       | The major version number                      | 1                          |
| <code>software_</code>                   | <i>int</i>       | The first minor version number                | 19                         |

| Field                                   | Type          | Description                     | Example                    |
|---|---------------|---------------------------------|----------------------------|
| version.minor                           |               |                                 |                            |
| software_<br>version.minor2             | <i>int</i>    | The second minor version number | 1                          |
| software_<br>version.minor3             | <i>int</i>    | The third minor version number  | 0                          |
| software_<br>version.version            | <i>string</i> | The full version string         | Wget/1.19.1<br>(linux-gnu) |
| software_<br>version.version_<br>number | <i>string</i> | The full version number         | 1.19.1                     |

[Back to top.](#)

[Back to Event Fields.](#)

## Observation fields

An `observation` event is created when the FortiNDR Cloud analytics backend identifies a correlation of information of interest. See below for valid values for the following fields:



You can view the list of observations in the *Observations* widget in the *Default Dashboard*. For more information, see:

- `observation_category`: asset, account, software, flow, file, relationship
- `observation_class`: anomalous, newly observed, specific



Observations run independently from the metadata extraction process, and are not tied to flow events with a `flow_id`. Additionally, an `observation` event may only have one of `src.ip` or `dst.ip`, although it could contain both.

The following table shows fields unique to the `observation` event type.

| Field                      | Type             | Description   | Example                      |
|----------------------------|------------------|---|------------------------------|
| evidence_end_<br>timestamp | <i>timestamp</i> | The timestamp for which the flagged activity ended. | 2019-01-<br>01T00:00:00.000Z |

| Field                    | Type                | Description   | Example  |
|--------------------------|---------------------|---|--|
| evidence_iql             | <i>string</i>       | An IQL statement that attempts to identify the events used to generate the observation.                           | src.ip = '10.10.10.10' AND customer_id = 'abc' AND dce_rpc:dce_rpc_operation = 'NetrSessionEnum' AND timestamp >= t'2019-01-01T22:00:00.000000Z' AND timestamp <= t'2019-01-01T22:10:00.000000Z' |
| evidence_start_timestamp | <i>timestamp</i>    | The timestamp for which the flagged activity began.   | 2019-01-01T00:00:00.000Z   |
| observation_category     | <i>string</i>       | The subject of an observation.  | relationship   |
| observation_class        | <i>string</i>       | The class of what was observed about the subject.   | specific   |
| observation_confidence   | <i>string</i>       | The confidence in the model output to what was attempted to be observed.  | high   |
| observation_title        | <i>string</i>       | The title of what was attempted to be detected - similar to a suricata sig name.                                  | High Count of NetSession Destinations  |
| observation_uuid         | <i>string</i>       | A unique identifier for the model used to generate the observation. Multiple models may exist for the same title. | ac33189b-ee31-4f5e-b6a1-dcb63d9a7295   |
| sensor_ids               | <i>string array</i> | A list of sensors from which activity was used as part of the observation.  | [abc1, abc2, abc3]   |

[Back to top.](#)

[Back to Event Fields.](#)

## Notice Fields

| Field       | Type               | Description                                 | Example |
|-------------|--------------------|---|---------|
| application | <i>application</i> | The classified application for a flow       |         |
| customer_id | <i>string</i>      | The code of the account that owns the event | chg     |



| Field              | Type                  | Description   | Example  |
|--------------------|-----------------------|---|--|
| dst_ip             | <i>string</i>         | The IP of the responder to the connection   | 8.8.8.8  |
| dst_ip_enrichments | <i>ip_enrichments</i> | Enrichments for an IP   |  |
| dst_port           | <i>integer</i>        | The port of the responder to the connection   | 53   |
| event_type         | <i>string</i>         | The type of event recorded  | flow   |
| file_desc          | <i>string</i>         | Description of a file to provide more context. For example, if a notice was related to a file over HTTP, the URL of the request would be shown. |  |
| file_mime_type     | <i>string</i>         | If the notice event is related to a file, this will be the mime type of the file.   |  |
| flow_id            | <i>string</i>         | A unique identifier for a flow shared by all events produced from that particular flow  | CtjvJR1nIzN4WFSuc7   |
| fuid               | <i>string</i>         | A file unique ID if this notice is related to a file.   |  |
| geo_distance       | <i>number</i>         | The difference between `src` and `dst` geo values   | 1410.373826280689  |
| intel              | <i>intel</i>          | Intel that matched entities in the event  |  |
| msg                | <i>string</i>         | Description of activity noticed.  | 10.1.0.47 appears to be guessing SSH passwords (seen in 30 connections). |
| n                  | <i>integer</i>        | Associated count, or perhaps a status code.   |  |
| note               | <i>string</i>         | Notice type   | SSH::Password_Guessing   |
| notice_actions     | <i>string</i>         | The actions which have been applied to this notice.   | [Notice::ACTION_LOG]   |
| peer_descr         | <i>string</i>         | Textual description for the peer that raised this notice, including name, host address and port.  |  |
| proto              | <i>string</i>         | The transport protocol.   |  |
| sensor_id          | <i>string</i>         | The sensor that created the event   | chg1   |
| source             | <i>string</i>         | The source of the event   | Zeek   |

| Field              | Type                  | Description   | Example                              |
|--------------------|-----------------------|---|--------------------------------------|
| src_ip             | <i>string</i>         | The IP of the initiator of the connection   | 10.10.10.10                          |
| src_ip_enrichments | <i>ip_enrichments</i> | Enrichments for an IP   |                                      |
| src_port           | <i>integer</i>        | The port of the initiator of the connection   | 52843                                |
| sub                | <i>string</i>         | Technical details of the activity.  |                                      |
| suppress_for       | <i>number</i>         | This field indicates the length of time that this unique notice should be suppressed. |                                      |
| tag                | <i>string</i>         | The type of event   | flow                                 |
| timestamp          | <i>string</i>         | The time at which traffic for the event began   | 2019-01-01T00:00:00.000000Z          |
| uuid               | <i>string</i>         | A unique identifier for the event   | 1ca116cb-9262-11e9-b5bf-02472fee9a4a |

[Back to top.](#)

[Back to Event Fields.](#)

## IQL Quick Reference

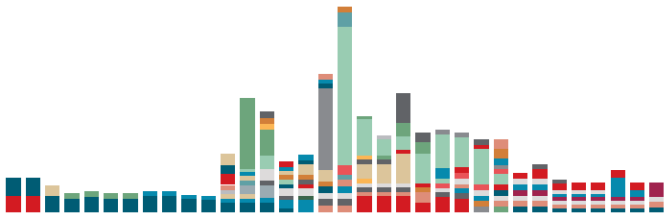
The *IQL Quick Reference* contains information and examples for creating IQL queries:

- [Network Security Posture Examples on page 42](#)
- [Hunt Examples on page 44](#)
- [Events and Properties on page 45](#)
- [Property Comparisons on page 46](#)
- [Querying Array/Nested Fields on page 47](#)
- [Building Complex Queries on page 48](#)
- [Aggregations on page 48](#)

## Network Security Posture Examples

### Cloud Storage Use Over Time

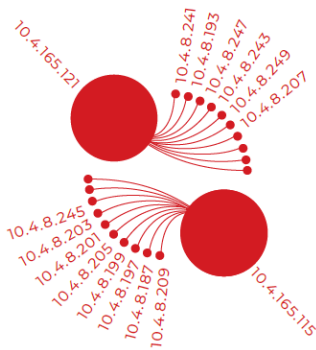
```
http:host MATCHES '.*(dropbox.com|\.box.com).*' GROUP BY HOUR(timestamp), src.ip
```



[Back to top.](#)

## Deprecated SSL Versions

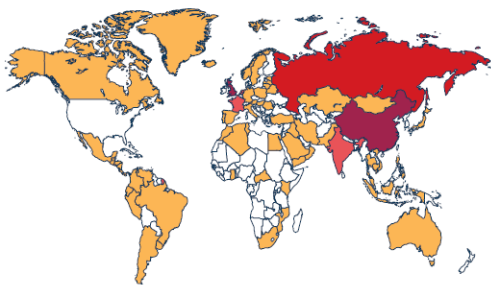
```
ssl:version MATCHES 'SSLv[2,3]|TLSv10' AND dst.internal = true AND src.internal = false  
GROUP BY dst.ip, src.ip
```



[Back to top.](#)

## Outbound SSH Sessions

```
src.internal = true AND dst.internal = false AND ssh:auth_success = true AND dst.asn.isp NOT  
IN ('Amazon', 'Amazon.com', 'GitHub, Inc.', 'GitHub') GROUP BY dst.geo.country,  
dst.asn.org
```

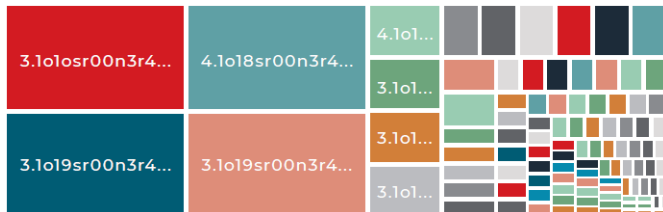


[Back to top.](#)

## Hunt Examples

### Long DNS Requests

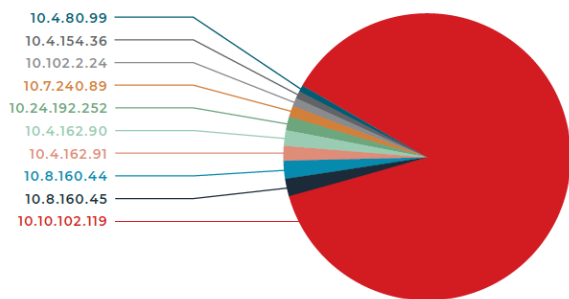
```
query.domain MATCHES '.{150,}' GROUP BY query.domain
```



[Back to top.](#)

### HTTP Post to IP Address

```
http:host.ip != null AND method = 'POST' AND dst.internal = false GROUP BY http:host.ip
```



[Back to top.](#)

### Possible Webshell Command Execution

```
src.internal = false AND ((uri.uri LIKE '%whoami%') OR (uri.uri LIKE '%netstat%') OR (uri.uri LIKE '%ifconfig%') OR (uri.uri LIKE '%ipconfig%')) AND status_code = 200 GROUP BY uri.uri
```

| uri.uri  | count |
|--|-------|
| /whoami  | 24    |
| /whoami?r=http://p.alocdn.com/c/3843/i/COOKIE_UID/p.gif                    | 19    |
| /users/610/visitors/whoami   | 5     |
| /live/boost/netstate/_ate.track.config_resp                                | 2     |
| /quiz-actions/a2536d84-7385-4003-82af-96f7ead2d71c/answers?apiAc-count=... | 2     |

[Back to top.](#)

## Events and Properties

### Event Types

- DCE-RPC
- DHCP
- DNS
- Flow
- FTP
- HTTP
- Kerberos
- NTLM
- Observation
- PE
- RDP
- SMB\_FILE
- SMB\_MAPPING
- SMTP
- Software
- SSH
- SSL
- Suricata
- TUNNEL
- X509

### Field Primitives

| TYPE      | SYNTAX                                  | EXAMPLES                      |
|-----------|---|-------------------------------|
| IP        | 8.8.8.8, '10.0.0.0/8',<br>"192.168.1.1" | ip, src.ip, answer.ip         |
| Timestamp | t'2017-02-08T17:49:10.017Z'             | timestamp pe_compile_time     |
| String    | 'www.google.com' "curl-agent"           | domain user_agent             |
| Integer   | 1234                                    | total_pkts total_ip_bytes     |
| Float     | 1.234                                   | duration geo_distance         |
| Boolean   | true false                              | src.internal has_export_table |

## Source and Destination

| PROPERTY                  | DESCRIPTION   |
|---------------------------|---|
| src.ip dst.ip             | IP address associated with the traffic  |
| src.port dst.port         | Port associated with the traffic  |
| src.ip_bytes dst.ip_bytes | Bytes transferred from the provided endpoint src.ip_bytes ==> uploaded                |
| src.pkts dst.pkts         | Packets transferred from the provided endpoint  |
| src.internal dst.internal | Boolean value defining whether the provided endpoint belongs to the customer IP space |
| src.asn dst.asn           | Registration information such as AS number and registered organization                |
| src.geo dst.geo           | Geolocation information such as city and country                                      |

[Back to top.](#)

## Property Comparisons

### Equal or Not Equal: = == != <>

#### Exact field match

```
dst.port = 80
event_type == "http"
domain == "www.google.com"
http:referrer = null (Records with no referrer)
ftp:dst.geo.country != 'US'
total_ip_bytes <> 0
http:host.ip != null (HTTP records accessed by IP)
```

### Less/Greater than (or equal to): < > <= >=

#### Filter on comparative size

```
timestamp > t"2017-01-01T00:00:00Z"
status_code < 500
duration <= 3600
duration <= 1 hour src.ip_bytes >= 1000000
bytes >= 1gb
```

### Set: IN

#### Exact match of multiple values

```
dst.ip IN ('8.8.8.8', '8.8.4.4')
http:method NOT IN ('GET', 'POST', 'CONNECT')
```

## Fuzzy: LIKE

Wildcards using SQL-like notation

% - 0 to many characters

\_ - One character

```
rdp:cookie LIKE "_"
http:user_agent NOT LIKE 'Mozilla%' ssh:cipher like '%RC4%' http:host.domain like
'%paypal%'.%.com
```

## Regex: MATCHES

(Formerly Lucene Regex support)

```
ssl:version MATCHES 'SSLv[2,3]|TLSv10'
user_agent NOT MATCHES '.*Chrome\/6[0-9]\..*'
query.domain matches '[a-zA-Z0-9]{16}\.onion((\.[a-zA-Z]+|([xX][nN]--[a-zA-Z0-9]+)))+)?'
```

[Back to top.](#)

## Querying Array/Nested Fields

### Nested Field Queries

| QUERY   | DESCRIPTION  |
|---|--|
| intel.feed = 'Alexa Top Domains' AND<br>intel.severity = 'high' | Filters on aggregated values on all intel objects. |
| intel {feed = 'Alexa Top Domains' AND<br>severity = 'high'}     | Filter on individual objects of intel field.       |



Scoped syntax, (i.e., using braces { }) only works for nested fields.

### List of Nested Fields

```
answers
files
headers.proxied_client_ips
intel
path
san_dns
san_ip to
uri.params
```

[Back to top.](#)

## Building Complex Queries

### Structural Components

- ( )
- AND
- OR

```
server_name MATCHES 'www\..*\.' AND subject MATCHES 'CN=www\..*\.' AND issuer MATCHES 'CN=www\..*\.'
```

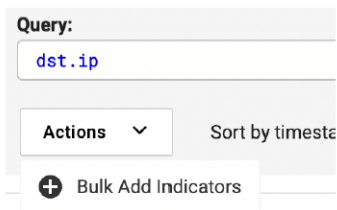
```
http:uri.uri LIKE '%.php?a=%&cd%&cr=%' OR uri.uri LIKE '%/?f=%&a=%&cd=%&cr=%&ir='
```

```
(http:user_agent='hola_get' OR http:host='client.hola.org') AND src.internal = true
```

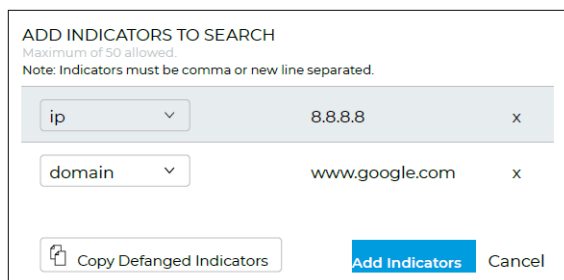
```
src.internal = true and (user_agent LIKE '%Windows_XP%' OR user_agent LIKE '%Windows 2003%' OR user_agent LIKE '%Windows NT 5.0%' OR user_agent LIKE '%Windows 2000%' OR user_agent LIKE '%Windows NT4.0%')
```

### Bulk Indicator Parsing

Quickly search across your environment for multiple indicators by pasting an unformatted text blob (or list of indicators) into the bulk indicator search feature. From the *Actions* menu, click *Bulk Add Indicators*:



FortiNDR Cloud will parse the contents for IoCs (IPs, domains, hashes, etc.), remove common defanging techniques and generate a query to run in your environment.



[Back to top.](#)

## Aggregations

Aggregate up to two fields using GROUP BY. Returns top 100 aggregate values of \$field1 and top 10 of \$field2. Modify counts using limit. Maximum of 10,000 aggregates.



## Unique Value Counting

```
src.internal = true AND dst.internal = false AND service = 'dns'
GROUP BY dst.ip
```

```
src.internal = true and http:host MATCHES '.*(gotomypc.com|logmein.com)' GROUP BY src.ip
limit 20, http:host limit 4
```

```
src.internal = true AND dst.internal = false AND service = 'http' GROUP BY src.ip limit
10000
```

## Aggregate Functions

### Sum

Sum of integer or float field

Sum of integer or float field

```
src.internal = true AND src.ip_bytes > 1000000000 AND dst.ip_bytes
< 500000000 AND dst.internal = false GROUP BY dst.asn.org, SUM(src.ip_bytes)
```

```
src.internal = true AND dst.asn.asn_org = 'Amazon.com, Inc.' GROUP BY src.ip, SUM(total_ip_
bytes)
```

### Min/Max

Min/Max value of integer, float, timestamp field

```
http:host.domain = 'lumtest.com' AND uri.uri = '/myip.json' AND referrer.host.domain = null
GROUP BY src.ip, MIN(timestamp)
```

```
service = 'ssh' AND src.internal = true AND dst.internal = false GROUP BY src.ip, MAX
(duration)
```

### Minute/Hour/Day

X-duration buckets of events based on any timestamp field

```
src.internal = true AND dst.internal = false AND flow:service != null GROUP BY HOUR
(timestamp), service
```

```
dst.asn.asn_org = 'Dropbox, Inc.' GROUP BY DAY(timestamp), sum(total_ip_bytes)
```

```
intel.indicator != null and dst.asn.asn_org in ('Hosting Solution Ltd.', 'Digital Ocean,
Inc.', 'Choopa, LLC') GROUP BY dst.ip, HOUR(timestamp)
```

## Key terms and concepts

| Term | Definition                         |
|------|------------------------------------|
| ATR  | FortiGuard Applied Threat Research |

| Term                        | Definition  |
|-----------------------------|---|
| <b>Detection</b>            | An alert mechanism that notifies you when a unique pair of events satisfy a rule. Detections allow you to quickly identify and respond to suspicious or known malicious activity in your network.   |
| <b>Detection lifecycle</b>  | The status states of a detection ( <i>Active</i> , <i>Muted</i> , or <i>Resolved</i> ).   |
| <b>Five-tuple (5-tuple)</b> | The source IP, source port, destination IP, destination port, and transport protocol. For more information, see <a href="#">Network events</a> .  |
| <b>Flow</b>                 | A collection of continuous packets having the same unique five-tuple (source IP, source port, destination IP, destination port, transport protocol) within a short time frame.  |
| <b>Indicators</b>           | An <i>indicator</i> is a field value extracted from a detection's event(s) as defined by the detection rule. This information is useful for identifying related activity and tracking indicators over time. Rules can define up to five fields to extract indicators from, and each detection can store up to five unique indicators for each indicator field.  |
| <b>MITRE ATT&amp;CK</b>     | <i>MITRE ATT&amp;CK</i> is a knowledge base of threat behaviors relied upon by security professionals worldwide. You can map FortiGuard Lab detection rules to MITRE ATT&CK, to enable visibility into the threat coverage provided by FortiNDR Cloud.  |
| <b>Rule</b>                 | A signature and other parameters used to detect something.  |
| <b>Tuning</b>               | The process of hiding known behaviors in a rule using one of the following three mechanisms: <ul style="list-style-type: none"><li>• <i>Muting</i>: Hides a detection but allows it to be created. Muted detections can be reviewed in bulk on a recurring basis. See <a href="#">Muting rules</a>.</li><li>• <i>Excluding</i>: Prevents detections from ever being created. Excluded detections cannot be reviewed in bulk on a recurring basis. See <a href="#">Excluding devices</a>.</li><li>• <i>Filtering</i>: Tuned out everything else, (such as external entities and non-entity fields) by adding your own logic to rules authored by FortiGuard Labs to customize the rule to your network. See <a href="#">Adding filters to rules</a>.</li></ul> |

# Dashboard

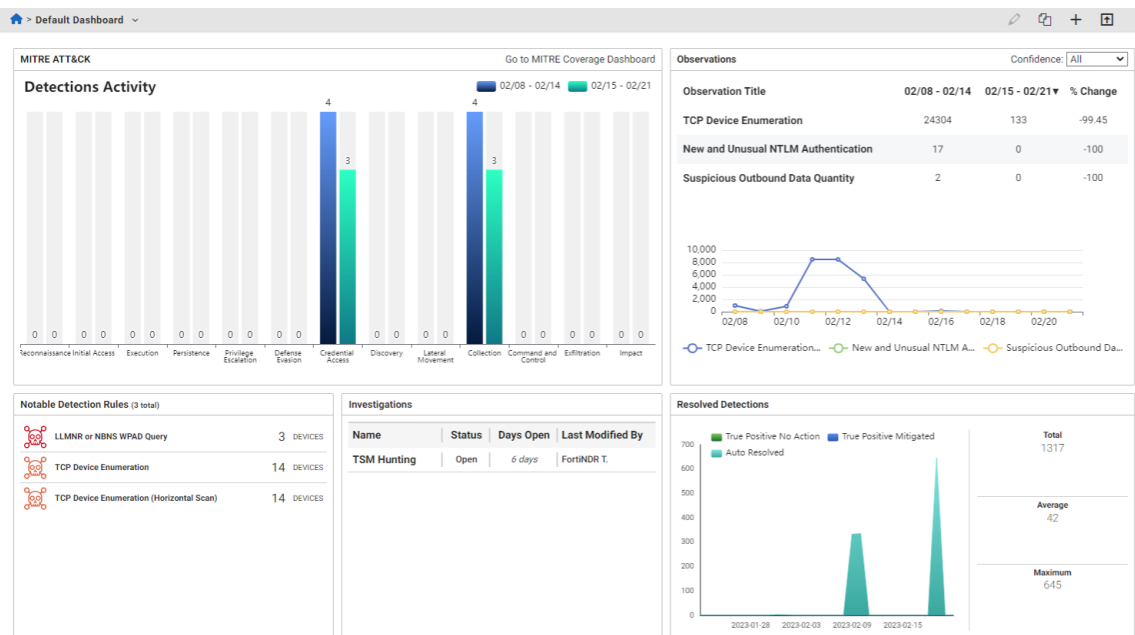
The Dashboard is the landing page for FortiNDR Cloud and provides an overview of detections activity, observations and investigations.

This section contains the following topics:

- [Default dashboard on page 51](#)
- [Observation detail page on page 52](#)
- [MITRE ATT&CK on page 54](#)
- [Viewing the MITRE ATT&CK Matrix on page 55](#)
- [Creating custom dashboards on page 56](#)

## Default dashboard

The default dashboard includes five widgets, most of which are focused on detection activity. You can use the dashboard as both an analytical and operational tool to view and act on the most important threats on your system.

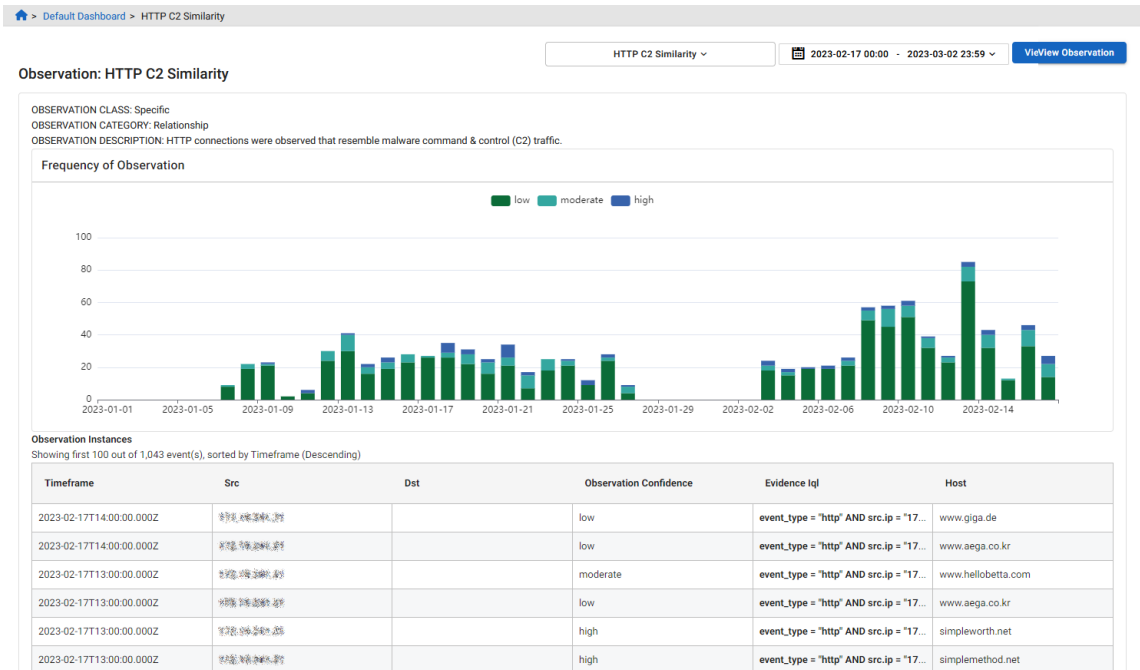


| Widget                  | Description  |
|-------------------------|--|
| <b>MITRE ATT&amp;CK</b> | <p>Detections are organized based on the MITRE ATT&amp;CK® framework.</p> <ul style="list-style-type: none"> <li>• There are two bars for every detection activity:               <ul style="list-style-type: none"> <li>• The left bar will show detections from previous time period.</li> <li>• The right bar will show detections from current time period.</li> </ul> </li> </ul> |

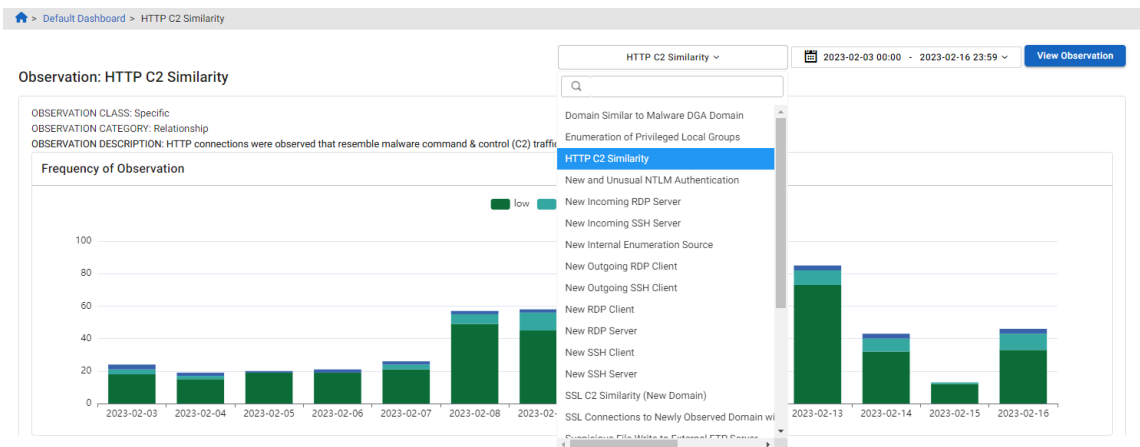
| Widget                         | Description   |
|--------------------------------|---|
|                                | <ul style="list-style-type: none"> <li>The column names may differ depending on the coverage on each account.</li> <li>Click the dates at the top of the widget to filter the chart by previous and current weeks.</li> <li>Hover over the bars in the chart to view the discover counts.</li> <li>Click the bars in the chart to open the <i>Detections Table</i>. See, <a href="#">Detections Table on page 86</a>.</li> </ul>  |
| <b>Observation</b>             | <p>Highlights observations (advanced correlations of multiple events by the FortiNDR Cloud backend.) Each observation will have different context variables that will show up.</p> <ul style="list-style-type: none"> <li>You can click the <i>Observation Title</i> to pivot to observation detail page.</li> <li>Each column header is clickable.</li> <li>Hover over the data points in the graph to view detailed information about the observation.</li> <li>Click the items in the legend to hide or show lines in the chart.</li> <li>Use the <i>Confidence</i> dropdown to filter observations based on the confidence level (<i>All, High, Moderate</i> or <i>Low</i>).</li> <li>Under <i>Observation Title</i>, click the individual observation titles to view the observation detail page. See <a href="#">Observation detail page on page 52</a>.</li> </ul> |
| <b>Notable Detection Rules</b> | Highlights active rules with the highest severity and detection count.  |
| <b>Investigations</b>          | <p>Highlights investigations with the most recent activity.</p> <ul style="list-style-type: none"> <li>The table is sorted by <i>Last Modified</i>. Any investigations that are modified appear at the top.</li> <li>Click <i>Investigations</i> to open the <i>Investigations</i> page. See <a href="#">Investigations on page 92</a>.</li> <li>Click an investigation name to open the <i>Investigation Details</i> page.</li> <li>Hover over <i>Last Modified By</i> or <i>Name</i> to view more information.</li> </ul>   |
| <b>Resolved Detections</b>     | <p>Displays daily resolved detection counts over time to highlight changes in activity (<i>Total, Average</i> and <i>Maximum</i>).</p> <p>You can click a data point in the chart or the <i>Total</i> detections, to view the resolved detections in the <i>Detections Table</i>.</p>   |

## Observation detail page

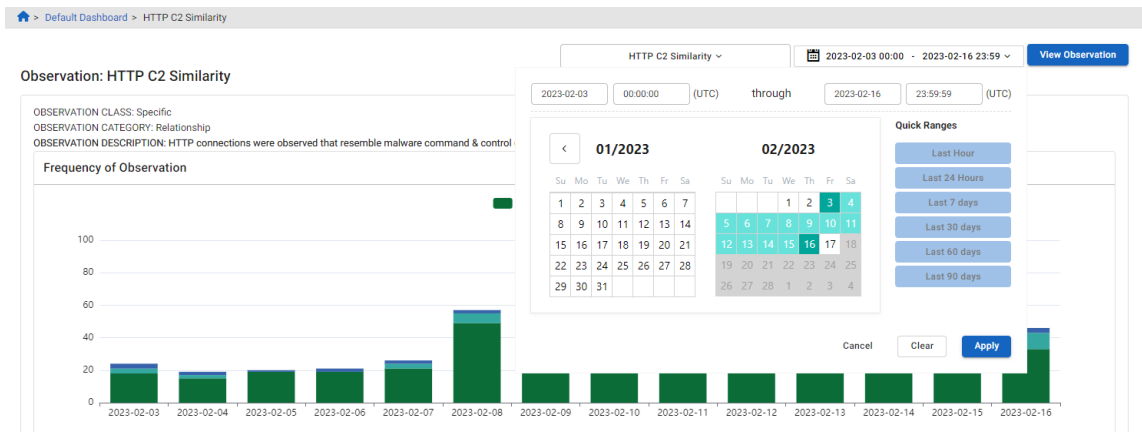
The Observation detail page displays drill-down information about the events that appear in the *Observations* widget. The Observations Instances table displays up to 100 observation instances (rows) even if there are more than 100 instances.



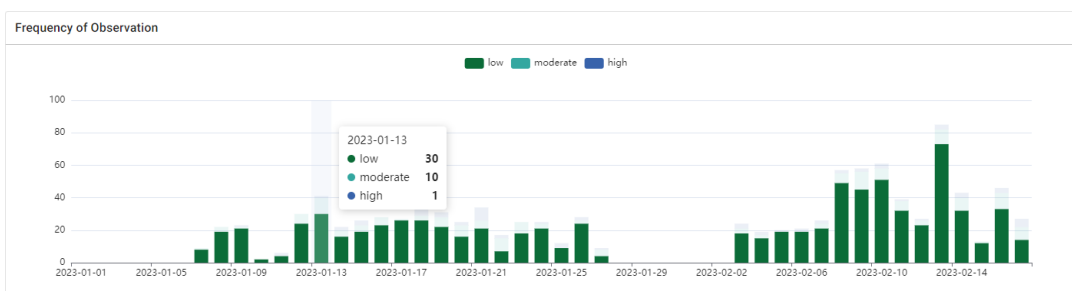
To switch to other observations available for your account, select a category from the drop-down and then click **View Observation**.



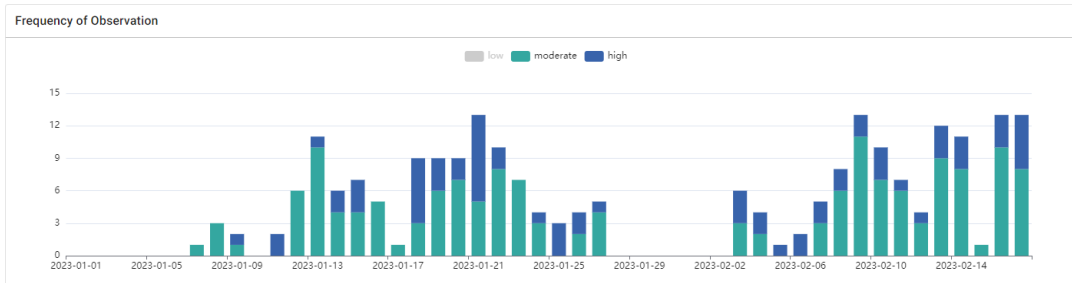
The table is sorted by *Timeframe* column in descending order. You can use the date pickers to configure the timeframe.



Hover over the graph to view the number of events by confidence level.



Click *Low*, *Moderate* or *High* to filter the table by confidence level.

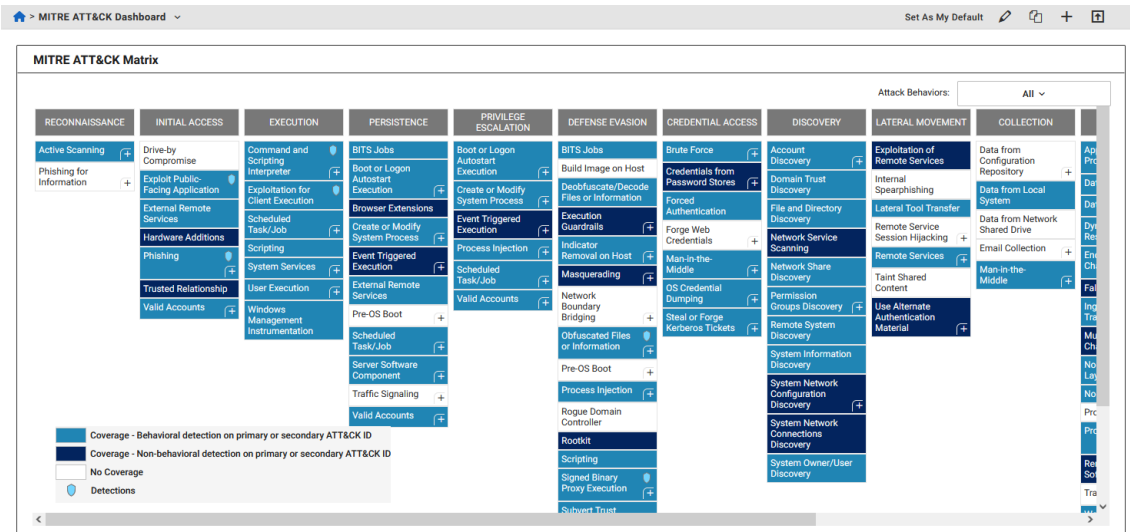


## MITRE ATT&CK

The *MITRE ATT&CK Matrix* dashboard shows detection coverage based on rules authored by FortiGuard Labs.

MITRE ATT&CK is a knowledge base of threat behaviors relied upon by security professionals worldwide. You can map FortiGuard Lab detection rules to MITRE ATT&CK, to enable visibility into the threat coverage provided by FortiNDR Cloud.

The dashboard displays the detection by behavior (behavioral and non-behavioral) and by technique (primary and secondary). The *Primary Technique*: is what is used to detect the behavior. The *Secondary Technique*: is not always related to what is seen on the network, but is related to the threat in general. The secondary technique will not be displayed in most instances.



## Viewing the MITRE ATT&CK Matrix

To view the MITRE ATT&CK Matrix:

1. Click the *Dashboard* tab.
2. In the toolbar at the top left-side of the page, click *Default Dashboard > MITRE ATT&CK Dashboard*. Optionally, you can click *Go to MITRE Coverage Dashboard* in the *MITRE ATT&CK* widget in the *Default Dashboard*.
3. Click the *Attack Behaviors* drop-down at the top-right of the dashboard to filter the dashboard by behaviors:
  - *All*
  - *Ransomware*
  - *Insider Threat*
  - *Cyber Espionage*
4. Click a technique in the table. A pop-up window displays a summary of the technique.

|                 |  |
|-----------------|--|
| <b>Tactic</b>   | The tactic of the behavior.  |
| <b>Coverage</b> | The coverage status of the technique and the sub-techniques.   |
| <b>Name</b>     | The behavior name.   |
| <b>ID</b>       | ID number of the technique and the sub-techniques.<br>For techniques and sub-techniques with active detections (indicated by a blue shield icon), the ID number is a hyperlink that directs you to the <i>Detections</i> page. |



The primary technique box displays a blue shield icon if there are active detections related to this technique or its sub-technique, and if you have the required permission to view the detections in the *Detection* page.

Techniques with an empty shield icon indicate that the detections are resolved. You can still view the detections in the *Detections* page.

Techniques without any past or present detections are displayed as text. However, it may also indicate that you do not have permission to view the detections related to the technique.

**Phishing** ×

**Tactic:** Initial Access  
**Coverage:** Behavioral detection on primary or secondary ATT&CK ID

---

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source.

| Name     | ID    |
|----------|-------|
| Phishing | T1566 |

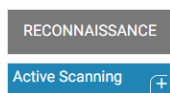
Sub-techniques (3)

| Name                      | ID        |
|---------------------------|-----------|
| Spearphishing Attachment  | T1566.001 |
| Spearphishing Link        | T1566.002 |
| Spearphishing via Service | T1566.003 |

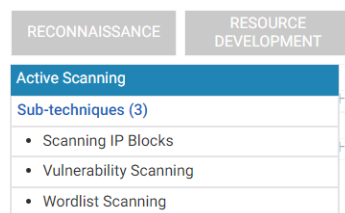
**Legend:**

- Coverage - Behavioral detection on primary or secondary ATT&CK ID
- Coverage - Non-behavioral detection on primary or secondary ATT&CK ID
- No Coverage
- Not visible by network analysis
- Detections

- To view the sub-technique, on the plus (+) symbol in the bottom-right corner of a Primary Technique box.



The box expands to show the sub-techniques.



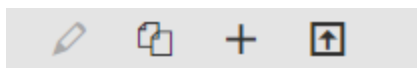
## Creating custom dashboards

Combine widgets to create custom dashboards. Custom dashboards are automatically updated approximately every five minutes. You can also set a custom dashboard as your default dashboard.

To switch between dashboards, click the *Default Dashboard* drop down in the toolbar, at the top left-side of the page.

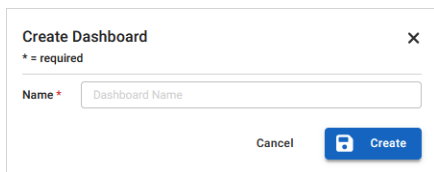
### To create a custom dashboard:

- Click the *Dashboard* tab.
- In the toolbar at the top right-side of the page, click *Add*. The *Create Dashboard* dialog opens.



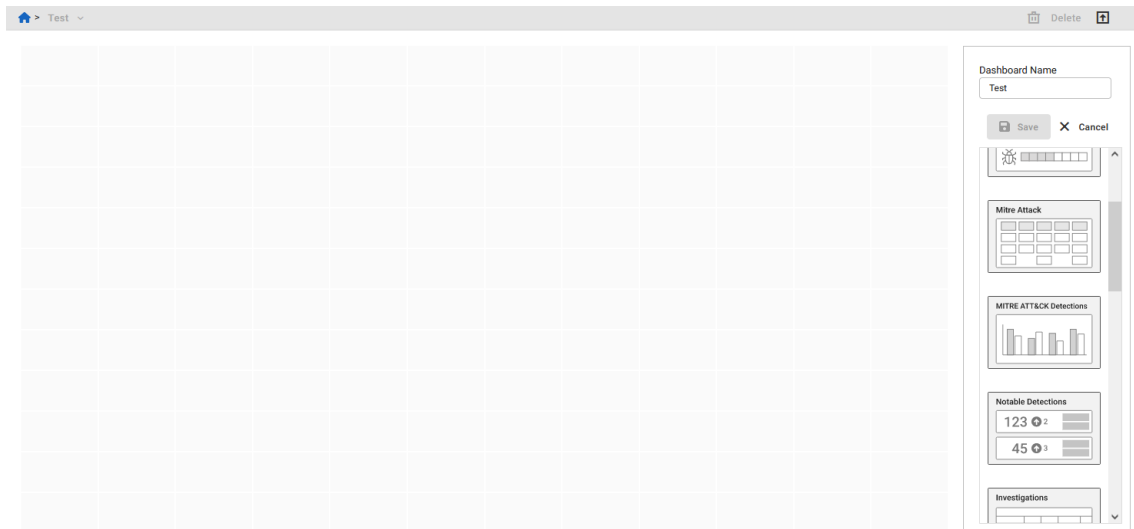


3. In the *Name* field, enter a name for the dashboard and click *Create*.



A dialog box titled "Create Dashboard" with a close button (X) in the top right corner. Below the title, it says "\* = required". There is a text input field labeled "Name" with "Dashboard Name" entered. At the bottom, there are two buttons: "Cancel" and "Create".

4. Drag and drop the widgets from the pane on the right side of the page onto the dashboard.



The dashboard editor interface shows a large grid on the left for placing widgets. On the right, there is a sidebar with a "Dashboard Name" field containing "Test", "Save" and "Cancel" buttons, and a list of widget thumbnails including "MITRE ATT&CK Detections", "Notable Detections" (with counts 123 and 45), and "Investigations".

5. Arrange the widgets on the dashboard and click *Save*.
  - To change the Block Name, click the edit icon.
  - To remove the widget from the dashboard, click the delete icon.



Each widget takes up a different amount of space. Some widgets may not fit onto one dashboard.

6. Click *Save*.

### To edit a custom dashboard

1. Click the *Dashboard* tab.
2. Click the *Default Dashboard* menu at the top left-side of the page and select a dashboard from the list.
3. In the toolbar, click the *edit* icon.



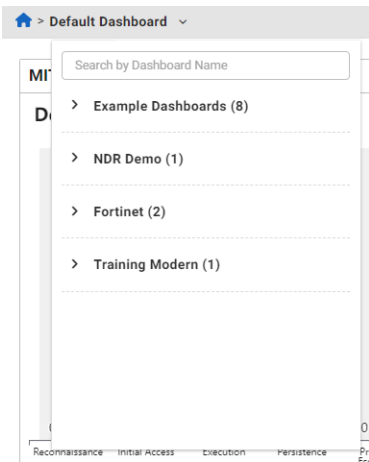
4. Edit the dashboard and click *Save*. The dashboard is added to the *Default Dashboard* drop down.



You cannot edit the default dashboard.

**To copy a dashboard:**

1. Click the *Dashboard* tab.
2. Click the *Default Dashboard* drop down at the top left-side of the page and select a dashboard from the list.



3. In the toolbar, click the *copy* icon. The *Copy Dashboard* dialog opens.
4. In the *Name* field, enter a new name for the dashboard.
5. In the *Account* drop down, select where the dashboard will appear in the menu.
6. Click *Copy*.



**To set a custom dashboard as the default:**

1. Click the *Dashboard* tab.
2. Click the *Default Dashboard* menu at the top left-side of the page and select a dashboard from the list.
3. In the toolbar, click the *Set as My Default*.



# Detections

FortiNDR Cloud *Detections* is an alert mechanism that notifies you when events matching a specific criteria appear in your account. Detections allow you to quickly identify and respond to suspicious or known malicious activity in your network.

The *Detections* page displays a list of *Rules* with active *Detections* in your account.

- A *Rule* is the signature and parameters used to identify activity in the network.
- A *Detection* is the actual occurrence of activity satisfying a rule.











Each row in the page displays a single rule with at least one active detection.

A Detection is created when an event matches a rule's signature. Detections are identified based on both the IP address and the Sensor ID to avoid issues with overlapping IP space. A duplicate detection is not generated if a detection already exists for the IP address and sensor ID pair. Instead, the *Last Seen* timestamp is updated and the event is added to the rule's *Latest Events*. This also resets the counter for the detection's *Resolution Period* if detections for the rule are set to resolve automatically.

By default the *Detections* page displays all *Active* rules in your account. Once all detections for a rule are resolved or muted, the rule's status is automatically updated from *Active* to *Idle*. You can create a filter to view all rules and detections regardless of their status.

🏠 > Detections > Rules

Detection Rules

| 27 Rules   |                       | Search                  | Severity                          | Order By         | Impacted Devices | Muted    | ⋮ |
|--|-----------------------|-------------------------|-----------------------------------|------------------|------------------|----------|---|
|  <b>Emotet Banking Trojan Download</b><br>CATEGORY: Attack: Installation                        | SEVERITY: <b>HIGH</b> | CONFIDENCE: <b>LOW</b>  | LAST SEEN: 2023-03-19 12:46 (UTC) | AUTHOR: NDR Demo | 1                | MUTED: 0 | ⋮ |
|  <b>Executable Binary or Script Download via Wget or cURL</b><br>CATEGORY: Attack: Installation | SEVERITY: <b>HIGH</b> | CONFIDENCE: <b>LOW</b>  | LAST SEEN: 2023-03-20 10:14 (UTC) | AUTHOR: Fortinet | 1                | MUTED: 0 | ⋮ |
|  <b>Trickbot Banking Trojan SSL Certificate</b><br>CATEGORY: Attack: Command and Control        | SEVERITY: <b>HIGH</b> | CONFIDENCE: <b>MOD</b>  | LAST SEEN: 2023-03-19 15:03 (UTC) | AUTHOR: Fortinet | 2                | MUTED: 0 | ⋮ |
|  <b>IcedID Banking Trojan HTTP GET Request</b><br>CATEGORY: Attack: Command and Control         | SEVERITY: <b>HIGH</b> | CONFIDENCE: <b>MOD</b>  | LAST SEEN: 2023-03-19 10:02 (UTC) | AUTHOR: Fortinet | 1                | MUTED: 0 | ⋮ |
|  <b>Trickbot HTTP Server Response</b><br>CATEGORY: Attack: Command and Control                  | SEVERITY: <b>HIGH</b> | CONFIDENCE: <b>HIGH</b> | LAST SEEN: 2023-03-19 13:52 (UTC) | AUTHOR: Fortinet | 2                | MUTED: 0 | ⋮ |
|  <b>Trickbot Staging Download</b><br>CATEGORY: Attack: Installation                             | SEVERITY: <b>HIGH</b> | CONFIDENCE: <b>MOD</b>  | LAST SEEN: 2023-03-19 14:09 (UTC) | AUTHOR: NDR Demo | 2                | MUTED: 0 | ⋮ |
|  <b>Trickbot Data Exfiltration</b><br>CATEGORY: Attack: Exfiltration                            | SEVERITY: <b>HIGH</b> | CONFIDENCE: <b>MOD</b>  | LAST SEEN: 2023-03-19 15:03 (UTC) | AUTHOR: NDR Demo | 2                | MUTED: 0 | ⋮ |
|  <b>Enumeration of Domain Objects</b><br>CATEGORY: Attack: Discovery                            | SEVERITY: <b>HIGH</b> | CONFIDENCE: <b>LOW</b>  | LAST SEEN: 2023-03-22 10:16 (UTC) | AUTHOR: Fortinet | 1                | MUTED: 0 | ⋮ |
|  <b>Qbot Payload Download</b><br>CATEGORY: Attack: Installation                                 | SEVERITY: <b>HIGH</b> | CONFIDENCE: <b>HIGH</b> | LAST SEEN: 2023-03-19 14:09 (UTC) | AUTHOR: Fortinet | 2                | MUTED: 0 | ⋮ |
|  <b>Trickbot HTTP Exfiltration</b><br>CATEGORY: Attack: Exfiltration                            | SEVERITY: <b>HIGH</b> | CONFIDENCE: <b>HIGH</b> | LAST SEEN: 2023-03-19 13:52 (UTC) | AUTHOR: Fortinet | 2                | MUTED: 0 | ⋮ |

The *Detections* page displays the following information:

|                 |  |
|-----------------|--|
| <b>Name</b>     | The rule name.   |
| <b>Category</b> | There are three categories for rules: <i>Attack</i> , <i>Potentially Unwanted Application (PUA)</i> , and <i>Posture</i> . Each category contains a more detailed subcategory. For more information, see <a href="#">Rule Categories</a> . |

**Severity**

The severity measures the potential impact to the confidentiality, integrity, or availability of information systems and resources if the activity is confirmed to be a true positive. Severity can be assigned to one of the following values:

| Severity        | Description   | Examples  |
|-----------------|---|---|
| <b>High</b>     | Significant to fair impact with the potential to spread or escalate | Malicious code execution, C2 communications, lateral movement, data exfiltration  |
| <b>Moderate</b> | Fair impact with minimal potential to spread or escalate            | Activity that could indicate malicious intent, untargeted attacks with unknown success, data leakage, subversion of security or monitoring tools                                      |
| <b>Low</b>      | Little to no impact expected  | Potentially unauthorized software, devices, or resource use, untargeted adware or spyware, compromise of a personal device or device on an untrusted network, insecure configurations |

**Confidence**

*Confidence* measures how likely events matching the rule's signature are indicative of the activity specified in the rule description. A rule's confidence indicates its minimum true-positive detection rate.

| Confidence      | Minimum True-Positive Rate |
|-----------------|----------------------------|
| <b>High</b>     | 90%                        |
| <b>Moderate</b> | 75%                        |
| <b>Low</b>      | 50%                        |

FortiGuard Lab assigns a rule's initial confidence based on its performance during testing. Once deployed, rules are monitored for changes in their true-positive detection rate, which is based on the resolution state chosen by an analyst when resolving a detection. Once a rule crosses a higher or lower threshold, it is reviewed to determine whether it should be tuned or whether the confidence should be modified.

**Last Seen**

The UTC date and time when the last known event tied to the rule was observed. This is useful when determining when the most recent change to a rule has occurred.

**Author**

The account that authored the rule.

**Impacted Devices**

The internal IP address in the `src.ip` or `dst.ip` fields used to generate detections. This field is configurable.

**Status**

By default, every detection is in an *Active* state upon creation. *Active* detections generate a notification (see [Manage subscriptions on page 136](#)), but *Muted* detections will not. Detections remain *Active* until they are resolved manually by an analyst or automatically based on the rule's *Resolution Period*. Once resolved, their status changes to *Resolved*.

| Detection State | Description  |
|-----------------|--|
| <b>Active</b>   | When an event matching a rule is observed, a detection is generated and set to Active by default. A notification is triggered for Active detections. |
| <b>Muted</b>    | When an event matching a rule is observed, but some aspect of it is muted. A notification is <i>not</i> triggered for Muted detections.              |
| <b>Resolved</b> | When a detection is resolved, either manually by an analyst or automatically, and is no longer Active.   |

## Rule Categories

| Category | Subcategory         | Description  |
|----------|---------------------|--|
| Attack   | Infection Vector    | Attacks in the initial stages before an exploit attempt has been made or malicious code has been executed. Examples include downloading a malicious executable file, navigating to a web site that is known to redirect to exploitation servers, or an attempt to authenticate to an SSH server from a malicious host.                                 |
| Attack   | Exploitation        | Attacks in the process of exploiting known vulnerabilities such as those listed in MITRE's Common Vulnerabilities and Exposures (CVE) list. While FortiNDR Cloud may be unable to determine the success of a launched exploit, any hosts attempting exploits (that are not approved internal scanners) should be investigated for signs of compromise. |
| Attack   | Installation        | Installation of malicious software (staging) for persistence in an environment. For example, the Cobalt Strike staging tool downloading a Beacon backdoor over HTTP in order to provide persistence on a compromised host and run further post-exploitation commands.  |
| Attack   | Lateral Movement    | Tools and techniques commonly used by attackers to pivot from a compromised host to other assets within the environment. Such tools may also be legitimately used by system administrators but should be investigated, especially for hosts from which this activity has not be observed before.   |
| Attack   | Command and Control | Command and control traffic between compromised hosts and attacker infrastructure.   |
| Attack   | Exfiltration        | Data exfiltration from compromised assets to external entities.  |

| Category | Subcategory                                 | Description  |
|----------|---|--|
| Attack   | Discovery                                   | Tools and techniques commonly used by attackers to identify accessible hosts and services. Such tools may also be legitimately used by system administrators but should be investigated, especially for hosts from which this activity has not been observed before.   |
| Attack   | Impact                                      | Malware or behavior intended to disrupt the business, such as distributed denial of service (DDoS) and ransomware attacks.   |
| PUA      | Adware                                      | Malware characterized by its use of advertisements to generate revenue for the author. Adware is often installed alongside third-party applications and remains on a system as a browser add-on or self-proclaimed optimization software. Most adware is considered low risk due to its innocuous nature.  |
| PUA      | Spyware                                     | Malware characterized by its focus on gathering device and user information without the user's knowledge. This information is usually sent back to the authors for a variety of purposes, ranging from market research to targeted monitoring. Spyware is usually installed alongside third-party applications and persists on a system as a backdoor or as software that purports to be useful. Most spyware is considered low risk due to its historical use for low-impact data collection and advertising.               |
| PUA      | Unauthorized Resource Use                   | Applications that utilize system resources without a user's knowledge or consent. Such applications are usually installed alongside third-party applications or as a component of malware in order to monetize a successfully compromised host (for example, via click fraud or cryptocurrency mining).  |
| Posture  | Potentially Unauthorized Software of Device | Applications or devices that circumvent organizational policies or increase the attack surface of an organization. These rules cover various applications that may be used to bypass monitoring tools and access controls, or store sensitive information in unauthorized locations. This category also includes tools that may be legitimately used for system administration, development, or penetration testing, but are also commonly used by attackers to enumerate access and pivot within a compromised environment. |
| Posture  | Insecure Configuration                      | Configurations within an environment that make it more vulnerable to exploitation or post-exploitation techniques used by attackers. Such configurations include outdated software, use of deprecated cryptographic standards, or configurations resulting in data leakage.  |
| Posture  | Anomalous Activity                          | Network activity that is abnormal and should be investigated to determine its cause. The activity may be malicious in nature or a misconfiguration that may or may not have security implications.   |

## Triage rules

The *Triage Rules* view is the landing page for the *Detections* tab. Use this view to review and respond to detections triggered by the rule.



**To view the Triage Rules page:**

1. Go to *Detections > Triage Rules*. The *Detections > Rules* page opens.
2. (Optional) Filter the rules on the page.

| <b>Search</b>             | Enter the technique ID, technique name or technique description.<br>Rules are filtered based on the prefix matching the selected technique ID. If Technique T1234 is entered, the rules returned include its sub-techniques T1234.001, T1234.002, T1234.003, etc.  |               |   |                 |  |                   |  |                  |   |                   |   |                         |   |               |   |             |  |              |  |                 |  |
|---------------------------|--|---------------|---|-----------------|--|-------------------|--|------------------|---|-------------------|---|-------------------------|---|---------------|---|-------------|--|--------------|--|-----------------|--|
| <b>Severity</b>           | Select High ( <b>H</b> ), Medium ( <b>M</b> ), or Low ( <b>L</b> ).  |               |   |                 |  |                   |  |                  |   |                   |   |                         |   |               |   |             |  |              |  |                 |  |
| <b>Additional Filters</b> | Click the filter icon to view additional filters.  |               |   |                 |  |                   |  |                  |   |                   |   |                         |   |               |   |             |  |              |  |                 |  |
|                           | <table border="1"> <thead> <tr> <th>Filter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>Category</b></td> <td>Filter the rules by category. See, <a href="#">Rule Categories</a>.</td> </tr> <tr> <td><b>Created By</b></td> <td>Filter by the account that created the rule.</td> </tr> <tr> <td><b>Technique</b></td> <td>Filter by the technique used for the detection.</td> </tr> <tr> <td><b>Confidence</b></td> <td>Select High (<b>H</b>), Medium (<b>M</b>), or Low (<b>L</b>).</td> </tr> <tr> <td><b>Detection Status</b></td> <td>Select <i>All</i>, <i>Active</i> or <i>Idle</i>.                             <table border="1"> <tr> <td><b>Active</b></td> <td>Rule has at least one Active (not Muted) detection.</td> </tr> <tr> <td><b>Idle</b></td> <td>Rule has zero Active (not Muted) detections.</td> </tr> </table> </td> </tr> <tr> <td><b>Muted</b></td> <td>Select <i>Unmuted</i> or <i>Muted</i>. See, <a href="#">Muting rules on page 66</a>.</td> </tr> <tr> <td><b>Disabled</b></td> <td>Select <i>Enabled</i> or <i>Disabled</i>. See, <a href="#">Disabling rules on page 69</a>.</td> </tr> </tbody> </table> | Filter        | Description   | <b>Category</b> | Filter the rules by category. See, <a href="#">Rule Categories</a> . | <b>Created By</b> | Filter by the account that created the rule. | <b>Technique</b> | Filter by the technique used for the detection. | <b>Confidence</b> | Select High ( <b>H</b> ), Medium ( <b>M</b> ), or Low ( <b>L</b> ). | <b>Detection Status</b> | Select <i>All</i> , <i>Active</i> or <i>Idle</i> . <table border="1"> <tr> <td><b>Active</b></td> <td>Rule has at least one Active (not Muted) detection.</td> </tr> <tr> <td><b>Idle</b></td> <td>Rule has zero Active (not Muted) detections.</td> </tr> </table> | <b>Active</b> | Rule has at least one Active (not Muted) detection. | <b>Idle</b> | Rule has zero Active (not Muted) detections. | <b>Muted</b> | Select <i>Unmuted</i> or <i>Muted</i> . See, <a href="#">Muting rules on page 66</a> . | <b>Disabled</b> | Select <i>Enabled</i> or <i>Disabled</i> . See, <a href="#">Disabling rules on page 69</a> . |
| Filter                    | Description  |               |   |                 |  |                   |  |                  |   |                   |   |                         |   |               |   |             |  |              |  |                 |  |
| <b>Category</b>           | Filter the rules by category. See, <a href="#">Rule Categories</a> .   |               |   |                 |  |                   |  |                  |   |                   |   |                         |   |               |   |             |  |              |  |                 |  |
| <b>Created By</b>         | Filter by the account that created the rule.   |               |   |                 |  |                   |  |                  |   |                   |   |                         |   |               |   |             |  |              |  |                 |  |
| <b>Technique</b>          | Filter by the technique used for the detection.  |               |   |                 |  |                   |  |                  |   |                   |   |                         |   |               |   |             |  |              |  |                 |  |
| <b>Confidence</b>         | Select High ( <b>H</b> ), Medium ( <b>M</b> ), or Low ( <b>L</b> ).  |               |   |                 |  |                   |  |                  |   |                   |   |                         |   |               |   |             |  |              |  |                 |  |
| <b>Detection Status</b>   | Select <i>All</i> , <i>Active</i> or <i>Idle</i> . <table border="1"> <tr> <td><b>Active</b></td> <td>Rule has at least one Active (not Muted) detection.</td> </tr> <tr> <td><b>Idle</b></td> <td>Rule has zero Active (not Muted) detections.</td> </tr> </table>  | <b>Active</b> | Rule has at least one Active (not Muted) detection. | <b>Idle</b>     | Rule has zero Active (not Muted) detections.                         |                   |  |                  |   |                   |   |                         |   |               |   |             |  |              |  |                 |  |
| <b>Active</b>             | Rule has at least one Active (not Muted) detection.  |               |   |                 |  |                   |  |                  |   |                   |   |                         |   |               |   |             |  |              |  |                 |  |
| <b>Idle</b>               | Rule has zero Active (not Muted) detections.   |               |   |                 |  |                   |  |                  |   |                   |   |                         |   |               |   |             |  |              |  |                 |  |
| <b>Muted</b>              | Select <i>Unmuted</i> or <i>Muted</i> . See, <a href="#">Muting rules on page 66</a> .   |               |   |                 |  |                   |  |                  |   |                   |   |                         |   |               |   |             |  |              |  |                 |  |
| <b>Disabled</b>           | Select <i>Enabled</i> or <i>Disabled</i> . See, <a href="#">Disabling rules on page 69</a> .   |               |   |                 |  |                   |  |                  |   |                   |   |                         |   |               |   |             |  |              |  |                 |  |
| <b>Order By</b>           | Order the rules by <i>Impacted Devices</i> , <i>Muted Devices</i> , <i>Severity</i> , <i>Confidence</i> , <i>Category</i> , or <i>Last Seen</i> .  |               |   |                 |  |                   |  |                  |   |                   |   |                         |   |               |   |             |  |              |  |                 |  |

3. Click a rule to open the *Details* page. The following information is displayed:

|                          |   |
|--------------------------|---|
| <b>Category</b>          | The attack category.  |
| <b>First Seen</b>        | The UTC date and time the first event associated with the detection occurred.   |
| <b>Last Seen</b>         | The UTC date and time of the last known event tied to the rule was observed.  |
| <b>Rule Updated</b>      | The UTC date and time the rule was modified.  |
| <b>Resolution Method</b> | <ul style="list-style-type: none"> <li>• <i>Automatic</i>: The detection will be resolved if events containing the same host and sensor ID are not observed for the specified time period.</li> <li>• <i>Manual</i>: The detection will remain active until an analyst resolves the detection.</li> </ul> |
| <b>MITRE ATT&amp;CK</b>  | The MITRE ATT&CK ID.  |

|                              |   |
|------------------------------|---|
| <b>Primary Technique</b>     | The primary attack name and ID.   |
| <b>Specificity</b>           |   |
| <b>Behaviors</b>             | The behavior coverage.  |
| <b>Description</b>           | A description of the detection.   |
| <b>Next Steps</b>            | Recommendations to resolve the detection.   |
| <b>Show Matching Events</b>  | Click to view the <i>Entity Lookup</i> .  |
| <b>Author</b>                | The rule author.  |
| <b>Impacted Device Field</b> | The fields used to generate the detection. The internal IP address in the <code>src.ip</code> or <code>dst.ip</code> fields is the default.   |
| <b>Indicator Fields</b>      | <p>The indicators the rule uses to generate the detection.</p> <hr/> <div style="display: flex; align-items: center;">  <p>This information is useful for identifying related activity and tracking indicators over time.</p> <p>Rules can define up to five fields to extract indicators from, and each detection can store up to five unique indicators for each indicator field.</p> </div> <hr/>   |
| <b>Impacted devices</b>      | <p>The active detections for the rule. All Active detections are displayed by default. You can create a filter to view Muted or Resolved detections.</p> <p>You can use this tab to resolve detections or to search for a device by IP.</p>   |
| <b>Signature</b>             | This tab displays the IQL signature defined for the rule. You can use a query string to create a custom rule. See, <a href="#">Adding custom filters to a rule signature on page 65</a> .   |
| <b>Events</b>                | <p>This tab displays all of the events that have matched the rule's signature.</p> <ul style="list-style-type: none"> <li>• Left-click on an entity to open the <i>Entity Panel</i>.</li> <li>• Right-click a field to open its menu (for example, <i>Search Events</i>, <i>Targeted Search</i> and <i>Copy to Clipboard</i>).</li> <li>• Hover a column header to lock, sort or arrange the columns.</li> </ul> <hr/> <div style="display: flex; align-items: center;">  <p>These events are duplicates of the original matching event. When an event matches a rule's signature, a copy is created and added to the rule's list of Latest Events so the event remains associated with the rule.</p> <p>This list can display up to the last 1000 matching events. Events could remain in the list in perpetuity if the rule rarely fires.</p> </div> <hr/> |
| <b>Indicators</b>            | <p>This tab displays the field value extracted from a detection's event(s) as defined by the detection rule.</p> <p>This information is useful for identifying related activity and tracking indicators over time. Rules can define up to five fields to extract indicators from and each detection can store up to five unique indicators for each indicator field.</p>  |



### Detections Graph

The *Detections Graph* plots a rule's detection volume over time. If a posture-related rule fires constantly, the graph will help show whether the issue is improving or worsening over time.

## Adding custom filters to a rule signature

You can customize a rule authored by FortiGuard Labs by adding an additional layer of logic to a signature. Filters extend the detection logic to account for differences specific to your network that muting and excluding do not account for.

### To add a custom filter to a signature:

1. Go to *Detections > Triage Rules* and open the rule.
2. Click the *Signature* tab.
3. Click *Add a Customer Filter*.
4. In the *Custom Filter* pane, enter a valid IQL string.



The query string needs to be true in addition to FortiGuard Labs's logic for a detection to be created. Similar to excluding, no detection will be created if an event is filtered by your custom logic.

The example below excludes traffic using a custom, internally defined `UserAgent` string.

The screenshot displays the configuration for a rule named "MS.IIS.Web.Server.Folder.Traversal.2". The rule is categorized as "Attack: Exploitation" and has a severity of "HIGH" and confidence of "HIGH". The "Signature" tab is selected, showing a complex IQL rule signature. A "Custom Filter" pane is open, containing the filter "user\_agent != 'ACME CORP - Custom Internal App v1.1'". The interface also shows "DEVICES IMPACTED" as 2 devices and 0 alerts.

5. Click *Test Filter*.
6. Click *Save Filter* to apply your logic to the rule.



To modify a custom query, click *Update Custom Filter* or click the delete icon above the *Custom Filter* pane.

## Search for a device hostname in rules

A Rule Signature does not allow for the inclusion of a device hostname in the rule logic. However, you can use a custom filter to search for a device by its hostname. For example, if there is a particular device hostname of interest in can be incorporated into a rule by creating a custom filter as shown below.

```
http:uri.path matches ". *W/[wN][iT][nN][nN][tT]V[ss][y~][ss][t T][eE](mM)32W/.(1,6)\. [eE][XX][eE].** and uri.path matches ". {0,4 0}?[\/] ([ss][cC][rR][it][pP][tT][sS][cc][gG][iTI]\-(bIiI1ΓnN)| [mM][s5] [aA] [dD][cC]|\_ [W][tT][iI]_[bB][it][nN]|\.(2))[\V/]L.[2].*
```

The screenshot shows a rule configuration page for 'MS.IIS.Web.Server.Folder.Traversal.2'. The rule signature is: `http:uri.path matches ". *W/[wN][iT][nN][nN][tT]V[ss][y~][ss][t T][eE](mM)32W/.(1,6)\. [eE][XX][eE].** and uri.path matches ". {0,4 0}?[\/] ([ss][cC][rR][it][pP][tT][sS][cc][gG][iTI]\-(bIiI1ΓnN)| [mM][s5] [aA] [dD][cC]|\_ [W][tT][iI]_[bB][it][nN]|\.(2))[\V/]L.[2].*`. A custom filter is added: `src.$device.hostname = 'FinanceWks008'`. The interface includes tabs for 'Impacted Devices', 'Signature', 'Events', 'Indicators', and 'Detections Graph'. It also shows 'DEVICES IMPACTED' as 2 devices and 0 alerts.



Only the "=", "!=", and "IN" filter conditions are supported for device hostname filters. Filter conditions such as "LIKE" and "MATCH" are unsupported.



The current Entity Tracking System only analyzes DHCP records. A custom filter leveraging a device hostname will only be as accurate as the available DHCP information.

## Muting rules

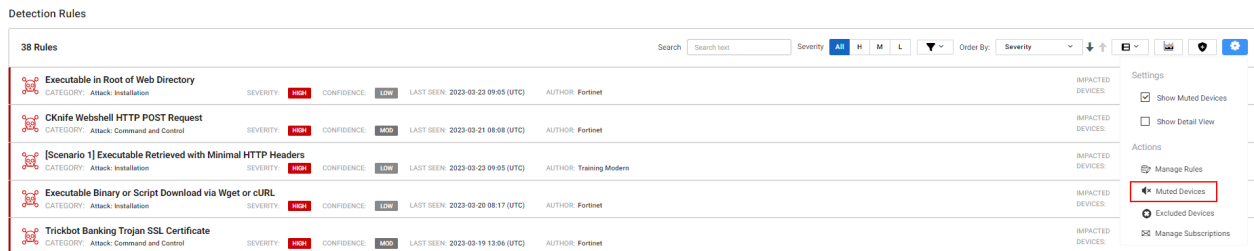
Muting allows you to ignore authorized and expected behaviors to identify anomalies for the specific host. When a rule is muted, any detection related to it has will have a status of *Muted*. This means a notification will not be generated for the detection. A muted detection will auto-resolve after the specified time frame or can be resolved manually.

### Mute all rules for devices

Muting a device for all rules. This is most commonly used for sandboxes and vulnerability scanners. These hosts will constantly trigger detections, while they are doing their job. Muting such devices is typically a first step when getting started with FortiNDR Cloud.

### To mute a device for all rules:

1. Click the *Detections* tab.
2. In the toolbar, click the gear icon at the right side of the page and select *Muted Devices*. The *Muted Devices* dialog opens.



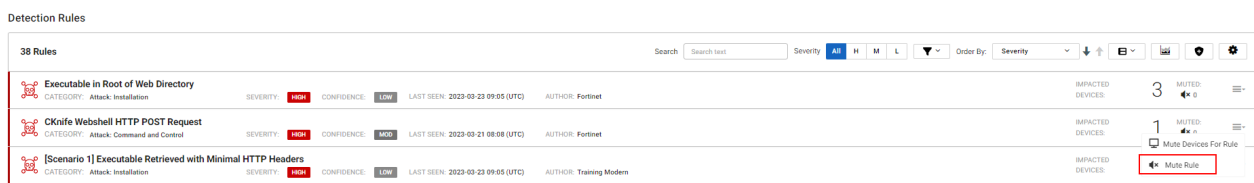
3. Click *Add New device Range*.
4. In the *Device IP or Range* field, enter an IP address or CIDR range.
5. Click *Add Devices*.

## Mute a rule

Muting a rule will cause all its future detections to be muted, regardless of the device that triggered the rule. Muting a rule is common for posture-focused rules that detect approved behavior.

### To mute a rule:

1. Click the *Detections* tab.
2. Click the menu icon at the right side of the page, and select *Mute rule*.



3. In the *Mute Rule* dialog that opens:
  - a. (Optional) In the *Comments* field
  - b. Click *Mute Rule*.

## Mute a detection in a rule

You can mute a specific device for a specific rule. This is commonly used for suspicious behaviors from approved devices, such as remote access from an administrator workstation. Detections that contain a muted rule are appended with *Muted* in the *Status* of column of the *Detections Table*.

### To mute a rule in a detection:

1. Click the *Detections* tab and open a rule in the list.
2. In the *Impacted Devices* tab, select the detection that contains the device and rule.

3. Click the *Actions* menu at the right side of the page and select *Mute device for rule*

The screenshot shows the FortiNDR interface for a detection rule titled "IcedID Banking Trojan HTTP GET Request". The rule is categorized as "Attack: Command and Control" and was updated on 2022-09-23 19:58 (UTC). The description states that the logic is intended to detect the banking trojan, IcedID, which hooks into users' browser sessions and can take screenshots. The "Next Steps" section lists five actions to take upon detection. Below this is a table of "Impacted Devices" with columns for Device IP, DHCP Ho..., Username, Hostname, MAC Address, Lifetime Events, Indicators, First Seen, Last Seen, Created, Updated, Sensor Id, Account, and Action. The first row shows a device with IP 10.10.31.101. The "Action" column for this device has a dropdown menu open, with "Mute Device for Rule" selected and highlighted with a red box.

4. In the *Mute Device* dialog that opens:
  - a. (Optional) In the *Comments* field
  - b. Click *Mute Rule*.



Alliteratively, you can go to *Detections > Detections Table*. In the Action column, click the menu and select *Mute device for rule*.

## Muting a device for an account


Muting a device for an account will add the device to your account's global device mute list.

### To mute a device for an account:

1. Go to *Detections* and open a rule. The *Impacted Devices* tab is displayed.
2. Click the *Actions* drop down at the right side of the page and select *Mute Device for Account*.
3. In the comments, explain why the device is muted.
4. Click *Mute Device*.

## Viewing muted devices

### To view muted devices:

| Option          | Description   |
|-----------------|---|
| Detection Rules | <ol style="list-style-type: none"> <li>1. Go to <i>Detections</i>.</li> <li>2. Click the <i>Settings</i> menu at the top-right of the page.</li> </ol>  <ol style="list-style-type: none"> <li>3. Under <i>Actions</i> select <i>Muted Devices</i>.</li> </ol> |

| Option                  | Description   |
|-------------------------|---|
| <b>Detections Table</b> | <ol style="list-style-type: none"> <li>Go to <i>Detections &gt; Detections Table</i>.</li> <li>Click the column selector and show the <i>Device Muted</i> column</li> </ol> |

## Excluding devices

You can exclude a device across all rules. This is useful in devices that are meant to perform functions that look suspicious out of context.



We recommend muting devices rather than excluding to allow for auditing and to have detections to reference if needed.

### To exclude devices:

- Click the Detections tab.
- In the toolbar, click the gear icon at the right side of the page and select *Excluded Devices*.

Home > Detections > Rules

Detection Rules

62 Rules

Search: Search text

Severity: All | H | M | L

Order By: Severity

| Rule Name  | Category                    | Severity | Confidence | Last Seen              | Author   | Impacted Devices  |
|--|-----------------------------|----------|------------|------------------------|----------|-------------------|
| Cobalt Strike Encrypted Beacon                         | Attack: Installation        | HIGH     | LOW        | 2023-02-16 12:05 (UTC) | Fortinet | IMPACTED DEVICES: |
| Executable in Root of Web Directory                    | Attack: Installation        | HIGH     | LOW        | 2023-02-16 13:12 (UTC) | Fortinet | IMPACTED DEVICES: |
| AZORult Check-in                                       | Attack: Command and Control | HIGH     | HIGH       | 2023-02-16 06:15 (UTC) | Fortinet | IMPACTED DEVICES: |
| Executable Binary or Script Download via Wget or cURL  | Attack: Installation        | HIGH     | LOW        | 2023-02-16 16:40 (UTC) | Fortinet | IMPACTED DEVICES: |
| Cobalt Strike Common Malleable Profile HTTP(S) Request | Attack: Command and Control | HIGH     | MED        | 2023-02-15 21:38 (UTC) | Fortinet | IMPACTED DEVICES: |

Settings:

- Show Muted Devices
- Show Detail View

Actions:

- Manage Rules
- Muted Devices
- Excluded Devices**
- Manage Subscriptions

< 1 2 ... 6 >

- Click *Add New device Range*.
- In the *Device IP or Range* field, enter an IP address or CIDR range.
- Click *Add Devices*

## Disabling rules

Disable a rule to exclude it from matching events. Disabling rules is useful for posture-focused rules that detect approved behavior

**To disable a rule:**

1. Go to *Detections*.
2. In the toolbar, click the gear icon at the right-side of the page and select *Manage Rules*. The *Manage My Rules* page opens.
3. In the *Actions* column, click the menu dropdown and select *Disable Rule*. A confirmation dialog opens.
4. Click *OK*.

## Resolving detections

You can resolve a detection to change its state from *Active* and remove it from the default view.

FortiGuard Labs curates detection rule logic over time. When the resolution ratio shows a high rate of False Positives, FortiGuard Labs will take steps to determine what changes are necessary in order to increase rule performance.



Detection resolutions are your direct feedback line to FortiGuard Labs. We recommend resolving detections to improve the quality of the rules you see.

**To resolve a detection:**

1. Click the *Detections* tab and open a rule in the list.
2. In the *Impacted Devices* tab, select the detection you want to resolve.
3. Click the *Actions* menu at the right side of the page and select *Resolve Detection*. The *Resolve <IP address>* dialog opens.
4. From the *Resolution* drop down, select one of the following options.

| Resolution State                | Description  | Example  |
|---------------------------------|--|--|
| <b>True Positive: Mitigated</b> | The threat was investigated and resolved, contained, or removed.             | Malware was discovered on a host.  |
| <b>True Positive: No Action</b> | The threat has been acknowledged, however no action was taken to resolve it. | An analyst ran a post-exploit tool for testing purposes.                         |
| <b>False Positive</b>           | The matched events don't represent the reported activity.                    | A signature for malware C2 instead flagged web browser traffic to a common site. |
| <b>Unknown</b>                  | The status or veracity of the detection is unknown.                          | You have no idea what you're even looking at, nor what to do with it.            |

5. (Optional) In the *Comments* field, enter brief description of the resolution.
6. Click *Resolve detection*.
7. (Optional) To unresolve a detection, select *Unresolve Detection* from the action menu.



Resolving a detection does not delete the detection, it simply removes it from the default view. Detections remain in your account in perpetuity and can be viewed or pulled via the API at any time.

To view resolved deflections, click the *Filter* button in the *Impacted Devices* tab on the Rule page and select *Resolved Detections*.

**To bulk resolve detections:**

1. Click the *Detections* tab and open a rule in the list.
2. In the *Impacted Devices* tab, click the select all box in the first column of the table. The *Bulk Resolve* icon is displayed.
3. Click *Bulk Resolve Detections*.



4. In the *Impacted Devices* tab, click *Bulk Resolve Detections*. the *Resolve X Detections* dialog opens.
5. From the *Resolution* drop down, select one of the following options.

| Resolution State                | Description  | Example  |
|---------------------------------|--|--|
| <b>True Positive: Mitigated</b> | The threat was investigated and resolved, contained, or removed.             | Malware was discovered on a host.  |
| <b>True Positive: No Action</b> | The threat has been acknowledged, however no action was taken to resolve it. | An analyst ran a post-exploit tool for testing purposes.                         |
| <b>False Positive</b>           | The matched events don't represent the reported activity.                    | A signature for malware C2 instead flagged web browser traffic to a common site. |
| <b>Unknown</b>                  | The status or veracity of the detection is unknown.                          | You have no idea what you're even looking at, nor what to do with it.            |

6. (Optional) In the *Comments* field, enter brief description of the resolution.
7. Click *Resolve detections*.


## Creating a rule

Create rules to monitor suspicious behavior on the network. You can create and store up to 50 detection rules per account. An error message appears when you reach the limit. We recommend reviewing your rules on a regular bases to ensure they are still in use. Consider deleting rules that are no longer in use. To increase the rule limit for an account, contact Customer Support.

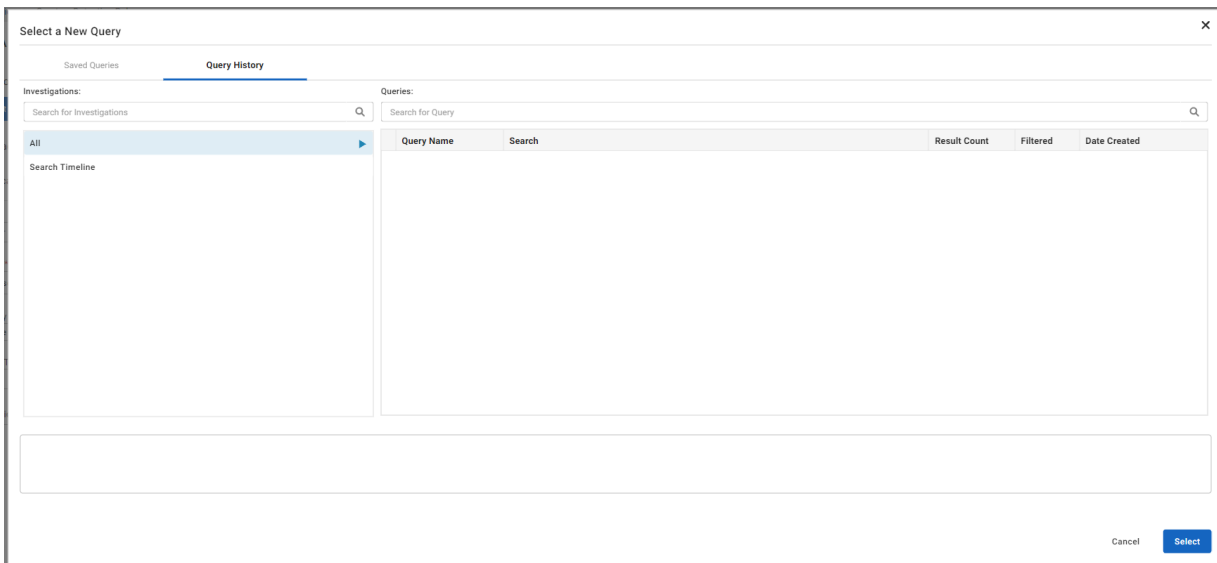


Before you create a rule, consider using a rule filter to customize a rule created by Fortinet. Rule filters save time creating a new rule and help manage the number of rules in your account. For information, see [Adding custom filters to a rule signature on page 65](#).

**To create a rule:**

1. Click the *Detections* tab.
2. In the toolbar at the top-right of the page, click the shield icon. The *Create A Detection Rule* page opens.
  - 
3. Click *Select New Query*. The *Select a New Query* dialog opens.
  - a. Click the *Saved Queries* or *Query History* tabs to create the new rule. Optionally, you can enter key words in the *Search for Query* field to search for a query.

- b. Choose a query from the list and click *Select*. To select an adhoc query, expand *Search Timeline*.



4. Configure the rule settings and click *Save Rule*.

|  |  |
|--|--|
| <b>Impacted Device IP can appear in the fields</b> | Click <i>Change Fields</i> to select the specific fields you want to use to generate a detection. By default, any internal IP address in the <code>src.ip</code> or <code>dst.ip</code> fields will be used to generate detections.  |
| <b>Indicators are captured in the fields</b>       | Click <i>Change Fields</i> to add or remove an Indicator Field for a rule. You can choose up to five fields.   |
| <b>Name</b>  | Enter a name for the rule.   |
| <b>Severity</b>                                    | Choose <i>High</i> , <i>Moderate</i> or <i>Low</i> .   |
| <b>Confidence</b>                                  | Choose <i>High</i> , <i>Moderate</i> or <i>Low</i> .   |
| <b>Category</b>                                    | Click the drop down to select a category from the list.  |
| <b>Primary Technique</b>                           | Enter the Primary Technique ID.  |
| <b>Secondary Technique</b>                         | Enter the Secondary Technique ID.  |
| <b>Run on Accounts</b>                             | Click <i>Manage Run List</i> to choose which accounts the new rule should run in.. In the dialog that opens, choose an account and click <i>Save</i> .<br>This is applicable only if you have access to multiple accounts. For example, if your organization acquired another organization, once you deploy sensors in their network, it might be easier to ingest that data into a separate account and give your team access to it. If you were to write a rule targeting specific subnets in your account, that rule wouldn't be applicable to the acquired company's network, so you would only want to deploy it in your account. |
| <b>Data Sources</b>                                | Enable/disable <i>Zeek</i> , <i>Fortinet</i> , <i>Zuricata</i> , or <i>Zscaler</i> .   |
| <b>Resolution Style</b>                            | Select <i>Auto</i> or <i>Manual</i> .  |
| <b>Automatic Resolution Period</b>                 | Select <i>6 hours</i> to <i>1 Month</i> .  |



Home > Detections > Create a Detection Rule

### Create A Detection Rule

Detection Rule Query:

[Select a New Query](#) Please select a previously run query to create a new detection rule.

Impacted Device IP can appear in the fields: **src.ip and/or dst.ip** [Change Fields](#)

Indicators are captured in the fields: [Change Fields](#)

Name \*

Severity \*  Confidence \*

Category \*

Primary Technique  Secondary Technique  Specificity

Description (Markdown Accepted)

Description Live Preview

Run on Accounts\*  
 Accounts: [IntelSec](#) [SignalStorm](#) [VirusShare](#)

Data Sources  
 Zeek  Fortinet  Suricata  Zscaler

Resolution Settings  
 Resolution Style  Automatic Resolution Period

[Cancel](#) [Save Rule](#)

## Start an investigation

### To start an investigation:

1. Go to *Detections > Triage Rules*. The *Detections Rules* page opens.
2. Click a rule to open the *Details* page.
3. Click *Start Investigation*. The *Add Query to Investigation* dialog opens.

|                                      |  |
|--------------------------------------|--|
| <b>Query Name</b>                    | Enter a name for the query.  |
| <b>Search Query</b>                  | Enter the query string.  |
| <b>Last 7 Days</b>                   | Click to set the data range to <i>Last Hour</i> , <i>Last 24 Hours</i> , <i>Last 7 days</i> , <i>Last 30 days</i> , <i>Last 60 days</i> or last <i>90 days</i> . |
| <b>Sort by timestamp</b>             | Select <i>Ascending</i> or <i>Descending</i> .   |
| <b>Retrieve up to</b>                | Click to set the number of rows retrieved ( <i>100</i> , <i>500</i> , <i>1000</i> , or <i>10,000</i> ).  |
| <b>Create a New Investigation</b>    | Click to create a new investigation.   |
| <b>Add to Existing Investigation</b> | The <i>Choose Investigation</i> dropdown is displayed. Select an investigation from the list.  |
| <b>Run a Private Query</b>           | Select this option to add a query to an adhoc search.  |

|                             |   |
|-----------------------------|---|
| <b>Investigation Name</b>   | Enter a name for the new investigation.             |
| <b>Description</b>          | Enter a short description of the new investigation. |
| <b>Choose Investigation</b> |   |

**Add Query to Investigation** ✕

---

Query Name:

Search Query:  
 ?

Retrieve up to  Rows  Enable Facets ⓘ

Create a New Investigation  
 Add to Existing Investigation  
 Run a Private Query

Investigation Name:

Description:

Cancel Add Query

4. Click *Add Query*.

## Viewing related investigations

**To view related investigations.**

1. Click the *Detections* tab and select a rule from the list.
2. Click *View Related Investigations*. The Investigations page opens.

## Running playbooks in a detection

Run a playbook used by the rule for a detection.

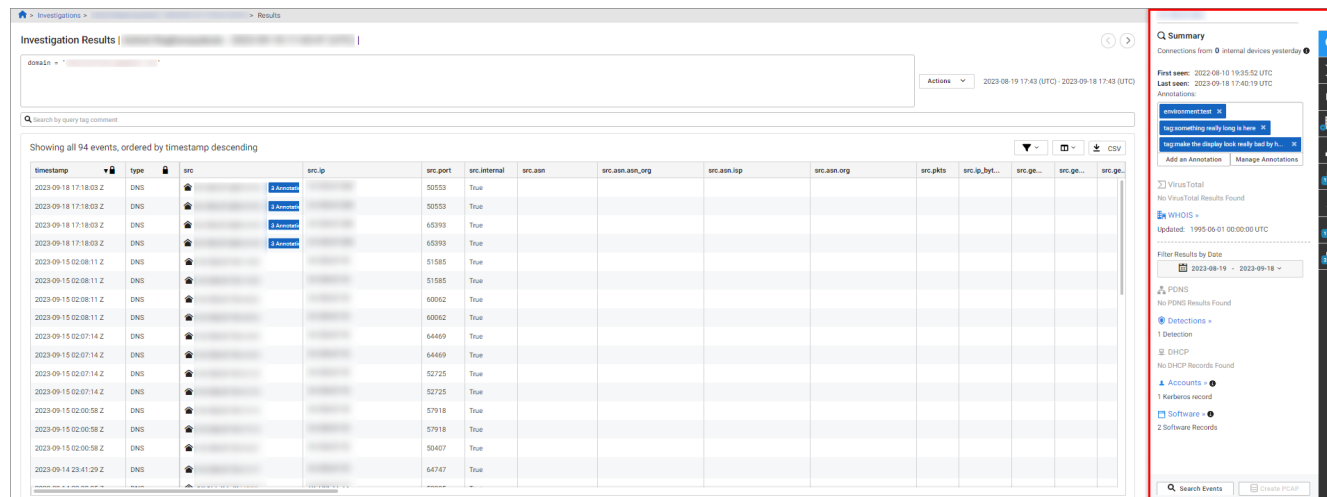
**To view a playbook in a rule:**

1. Click the *Detections* tab and open a rule in the list.
2. Click the *Events* tab.
3. In the *Timestamp* column, right-click an entry and select *Playbooks*. The *Add Playbook* page opens.
4. Select a playbook in the list.
5. Click *Run Playbook*.

## Entity Panel

An *Entity* is a unique identifier on the network. At this time, FortiNDR Cloud supports IP addresses and domains as entities. Entities are extracted from event data and cataloged in their own data store.

The *Entity Panel* displays the contextual information collected for an entity from within and outside the network. You can access the Entity Panel for an entity by clicking an IP address in the rule details tabs or clicking *View Device Details* in the Actions menu.



The Entity Panel is organized into tabs, which are listed on the right side of the page.

|                   |  |
|-------------------|--|
| <b>Summary</b>    | Shows the first and last seen timestamps, applied tags, and a summary of records on subsequent tabs.   |
| <b>WHOIS</b>      | Populated by FortiNDR Cloud WHOIS.   |
| <b>VirusTotal</b> | Populated by FortiNDR Cloud integration with VirusTotals details for: <ul style="list-style-type: none"> <li>• <i>Detected URLs</i>: A URL that returned results.</li> <li>• <i>Resolved URLs</i>: VirusTotal passive DNS resolution results.</li> <li>• <i>Communicating Samples</i>: Hashes of files that called out to the entity during dynamic analysis.</li> <li>• <i>Downloaded Samples</i>: Hashes of files that were downloaded from the entity during dynamic analysis.</li> <li>• <i>Referrer Samples</i>: Hashes of files that referred to the entity, but may have not communicated directly, during dynamic analysis.</li> </ul>         |
| <b>PDNS</b>       | <p>All passive DNS records observed for the entity for the life of the account. Two sets of data are displayed: <i>DNS record in the time range</i> and <i>Passive DNS record all time</i>.</p> <p>Records are displayed in the order they were last seen. The records within the time range appear at the top of the list. Records within the time range are highlighted by <i>First in Time Range</i> and <i>Last in Time Range</i>.</p> <p>The <i>Type</i> field indicates if the DNS type such as IPv4 (<i>a</i>), IPv6 (<i>aaaa</i>), canonical name (<i>CNAME</i>), name server (<i>NS</i>), mail exchange (<i>MX</i>), and text <i>TXT</i>.</p> |
| <b>Detections</b> | All FortiNDR Cloud detections observed for the entity for the life of the account.   |

|                    |   |
|--------------------|---|
| <b>Accounts</b>    | Kerberos and NTLM records observed for the entity over the past 30 days, particularly useful for identifying the users of an internal asset.  |
| <b>DHCP</b>        | All DHCP records for the entity for the life of the account.  |
| <b>Software</b>    | All software associated with the entity, observed from any network protocol.  |
| <b>FortiGuard</b>  | Indicates a malicious file is detected, with the message <i>File identified as malicious</i> . Click the section header or the FortiGuard icon to view the attributes about the malicious file. If the attributes are not available, then none are displayed. See <a href="#">To view malicious files with FortiGuard</a> . |
| <b>FortiEDR</b>    | This tab appears when the FortiEDR integration is enabled. For more information see, <a href="#">FortiEDR integration for FortiNDR Cloud</a> .  |
| <b>Crowdstrike</b> | This tab appears when the Crowdstrike integration is enabled. For more information see, <a href="#">CrowdStrike Falcon integration for FortiNDR Cloud</a> .   |

## Adding annotations and viewing malicious files

### To add an annotation:

1. In the *Summary* tab click *Add an Annotation*. The *Create an annotation* dialog opens.
2. From the *Select an annotation type* drop-down, select the annotation type.
3. In the *Enter an annotation name* field, enter a name for the annotation.
4. In the *Enter a description* field, enter the annotation.
5. Click *Save*. The annotation is added to the *Summary* tab.



For information about managing annotations, see [Manage Annotations on page 137](#).

### To view malicious files with FortiGuard:

1. In the investigation results, click the link in the *File* column.
2. Click a link in the *Files* dialog.
3. The *FortiGuard* area displays the *File identified as malicious* flag.

## Date ranges

Keep the following considerations in mind when view viewing results with the date range picker.

### Summary tab

- The date range picker is displayed In the *Summary* tab. The results in each section above the dashed line (*Detections*, *DHCP*, *Account* and *Software*) is captured within this date range. The information below the dashed line is independent from this date range.
- Sections in the Summary tab that use the date picker (such as DHCP) will also display the date picker in the corresponding tab.

|                           |  |
|---------------------------|--|
|                           | <ul style="list-style-type: none"> <li>The date range picker in any tab is global. If you change the start and end date in one tab it will change the date range everywhere in the panel.</li> </ul>   |
| <b>Date out of range</b>  | <ul style="list-style-type: none"> <li>The <i>Account</i> and <i>Software</i> tabs only display results for last 90 days. If the date picker end date exceeds 90 days, <i>Date out of range</i> is displayed.</li> </ul>   |
| <b>Default time range</b> | <ul style="list-style-type: none"> <li>The date range on Entity Panel defaults to the time range based on the page the panel is opened in. <ul style="list-style-type: none"> <li>The time range in the Entity Panel matches range when opened from the following pages: <ul style="list-style-type: none"> <li>Entity Lookup</li> <li>Visualizer</li> <li>Detection Table</li> <li>Sensor Visibility</li> <li>Investigate Results</li> <li>Adhoc Search</li> <li>Observation Detail</li> </ul> </li> <li>Detections is default to last 7 days when opened from the following pages: <ul style="list-style-type: none"> <li>Detection page</li> <li>Detection-Indicator page</li> <li>Detection-Triage Page</li> </ul> </li> </ul> </li> </ul> |

## Accessing the Entity Panel

You can access the Entity Panel from the following pages:

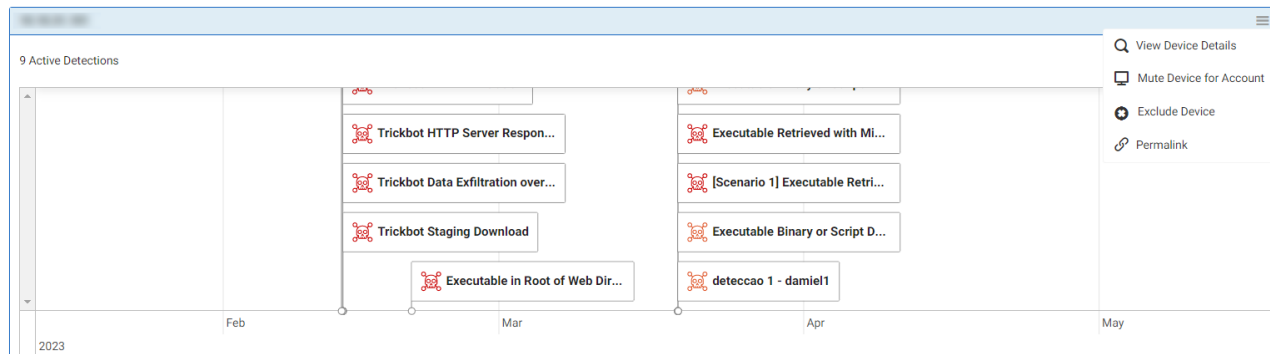
- Investigation Results: Click an IP address in the *Results* table.
- Observation : In the Dashboard > Observation details
- Adhoc Search Results
- Visualizer
- Detection Table
- Detection Triage Rule
- Detection Triage Devices
- Entity Lookup
- Detection Event Indicator
- Visible Device Page (Sensor)

## Get a permalink for a device

You can get a permalink to an affected device to share with members of your organization.

### To get a permalink:

1. Go to *Detections > Triage Devices*.
2. Click the Actions menu in the banner at the top of the page and select Permalink. The link is copied to your clipboard.



## Device Triage

Use the *Device Triage* page to review and respond to detections based on the risk score associated with a device. This page highlights the most critically impacted assets in your environment. Each section of the page offers a different perspective of active detections to help focus on what devices may deserve higher urgency.

The *Device Triage* page is organized into three panes:

### Impacted devices

*Impacted Devices*, located in the left-side pane helps you prioritize your triage process. Devices are displayed by their IP address, hostname, and Risk Score on a scale between 1-10 where 1 indicates low risk and 10 indicates high risk. The score is calculated from currently active detections of a device and is intended to be used in conjunction with your knowledge of the environment. Devices are ordered from high to low risk and can be searched, filtered, and sorted.

### Detection timeline

The *Detection Timeline* is located in the pane at the top of the page and displays a timeline of detections for each impacted device. To view the timeline for an impacted device, click the device in the *Impacted Devices* pane. The timeline will automatically scale to show all active and unmuted detections associated with the device. Click the filter button in the top right of the timeline to include muted or resolved detections in the timeline. You can drag the timeline left and right or zoom by scrolling over it to explore detections over time.

### Detection rules

*Detection rules* are located in the pane at the bottom of the page. The rules are sorted by severity by default. To view more information about a detection rule in the listed, click the rule title to open the rule details pane within the pane.

**Detections Triage**

**Impacted Devices**

Search by Device IP

- Hostname: N/A Risk Score: 10.0
- Hostname: enterprise-web Risk Score: 10.0
- Hostname: Enterprise-DC01 Risk Score: 10.0
- Hostname: Account@WU04 Risk Score: 10.0
- Hostname: Finance@WU08 Risk Score: 10.0
- Hostname: Developer@WU16 Risk Score: 8.0
- Hostname: N/A Risk Score: 7.6
- Hostname: N/A Risk Score: 4.1
- Hostname: Balise-PC Risk Score: 2.5
- Hostname: N/A Risk Score: 0.1

12 Active Detections

| Detection Rule  | Category                   | Severity | Confidence | First Seen             | Last Seen              | Status | Actions |
|---|----------------------------|----------|------------|------------------------|------------------------|--------|---------|
| [Scenario 1] Trickbot Data Exfiltration over SSL            | Attack-Exfiltration        | HIGH     | MED        | 2023-03-19 11:29 (UTC) | 2023-03-19 11:29 (UTC) | Active |         |
| ETERNALBLUE Exploitation                                    | Attack-Exploitation        | HIGH     | MED        | 2023-03-19 10:50 (UTC) | 2023-03-19 11:17 (UTC) | Active |         |
| [Scenario 1] Executable Retrieved with Minimal HTTP Headers | Attack-Installation        | HIGH     | LOW        | 2023-03-19 10:49 (UTC) | 2023-03-19 11:24 (UTC) | Active |         |
| Executable Retrieved with Minimal HTTP Headers              | Attack-Installation        | HIGH     | LOW        | 2023-03-19 10:49 (UTC) | 2023-03-19 11:24 (UTC) | Active |         |
| Executable in Root of Web Directory                         | Attack-Installation        | HIGH     | LOW        | 2023-02-20 09:49 (UTC) | 2023-03-19 10:49 (UTC) | Active |         |
| Trickbot Staging Download                                   | Attack-Installation        | HIGH     | MED        | 2023-02-13 10:39 (UTC) | 2023-03-19 11:39 (UTC) | Active |         |
| Trickbot Data Exfiltration over SSL                         | Attack-Exfiltration        | HIGH     | MED        | 2023-02-13 10:29 (UTC) | 2023-03-19 11:29 (UTC) | Active |         |
| Trickbot HTTP Server Response                               | Attack-Command and Control | HIGH     | MED        | 2023-02-13 10:09 (UTC) | 2023-03-19 11:09 (UTC) | Active |         |
| Trickbot HTTP Exfiltration                                  | Attack-Exfiltration        | HIGH     | MED        | 2023-02-13 10:01 (UTC) | 2023-03-19 11:09 (UTC) | Active |         |
| Trickbot Banking Trojan SSL Certificate                     | Attack-Command and Control | HIGH     | MED        | 2023-02-13 09:49 (UTC) | 2023-03-19 13:06 (UTC) | Active |         |

## Visualizer

Go to *Detections > Visualizer* to view detections data from existing APIs in a graphical interface. You can use the Visualizer to view the relationship between the rules and devices, inspect rules and impacted device detail, and navigate to the node view from the list of impacted nodes.

The visualizer will initially display all active, unmuted detections over the past 30 days in graphical form with nodes representing impacted devices and rules.

**Visualizer**

Nodes | Rule Name | 2023-01-17 - 2023-02-16 | PNG

**LEGEND:**

- Impacted Device (Blue circle)
- Indicators (Blue diamond)
- Rule/Severity (Red and Yellow hexagons)
- Muted (Red dashed line)
- Resolved (Grey line)
- Repeat Offender (Red hatched line)

**Indicators:** IPs, Files, Domains, Other

**Rule/Severity:** Attack, Posture, PUJA, Misc.

**MUTED:** Muted

## Filtering the Visualizer

Use the filters at the top of the visualizer to change the content displayed in the canvas. Some filter options are static, others are dynamic based on the criteria selected elsewhere. When you modify the filter, the graph will be redrawn per the selected options.



The Visualizer can retrieve up to 10,000 detections from the API regardless of the filter criteria.

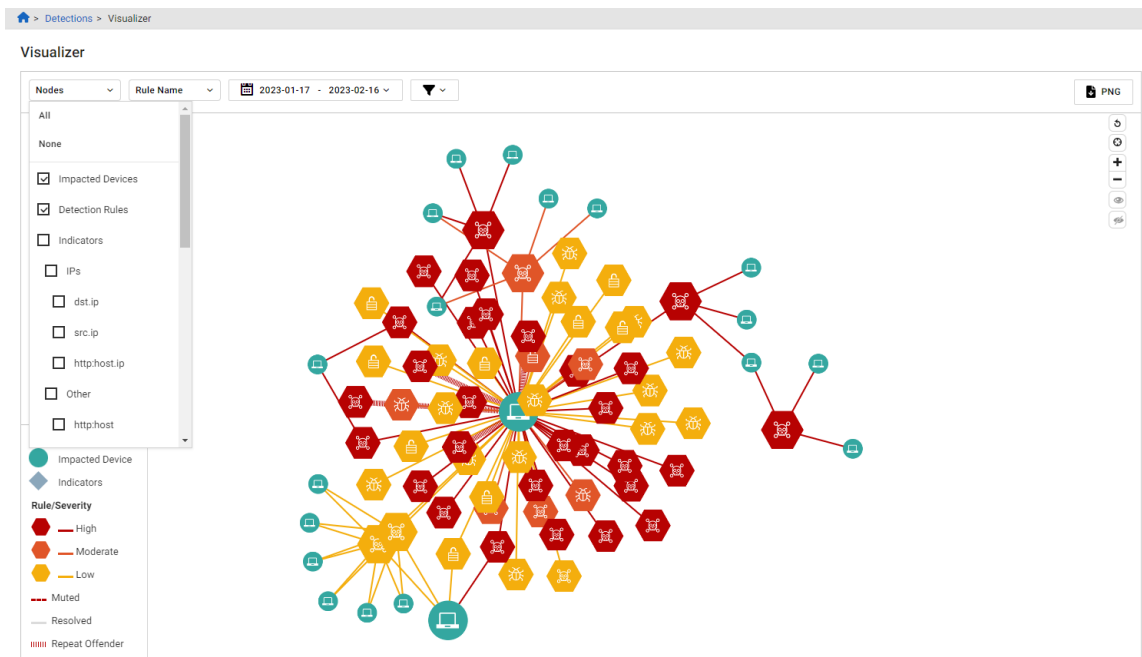
## Nodes

Use the *Nodes* filter to select the types of nodes to display. There are three types of nodes:

- Indicators
- Impacted Devices
- Detection Rules



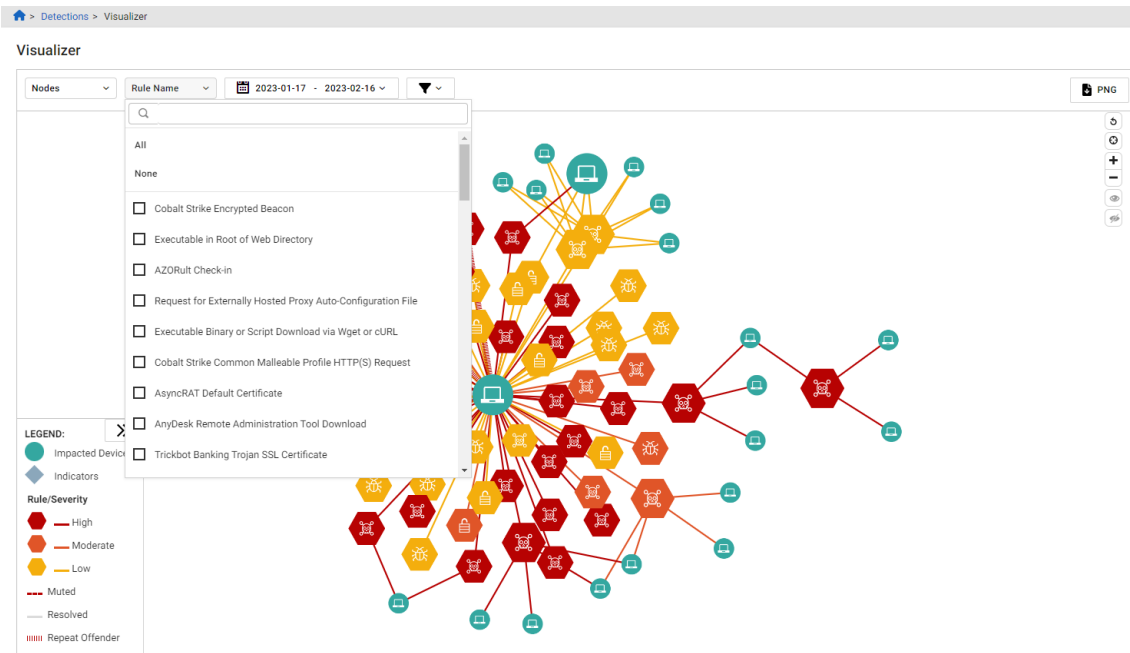
When the *Indicators* option is selected, groups of indicators and impacted devices related to the same rule may be clustered together on the graph. While any combination can be selected, omitting *Detection Rules* will usually result in a disjointed graph.





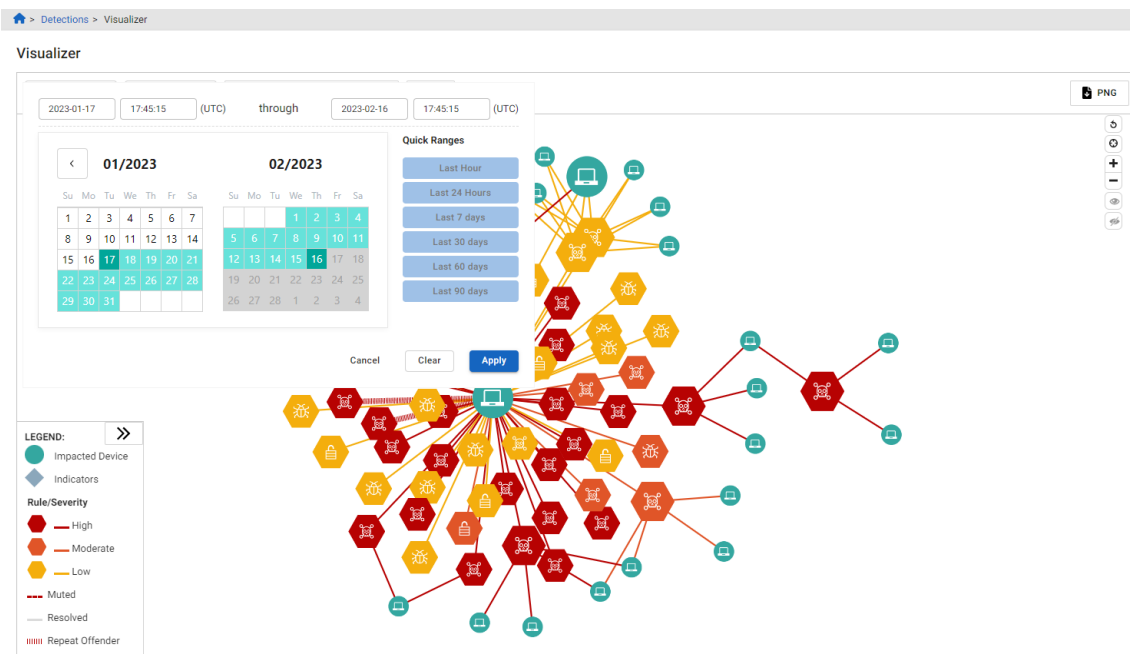
## Rule Name

Use the *Rule Name* filter to hide or display rules. The rules displayed will depend on the other criteria selected in the report. Only the rules that are relevant to the rest of the criteria (such as *Date Range*, *Device/Detections/Rule Status*, *Severity*) can be selected.



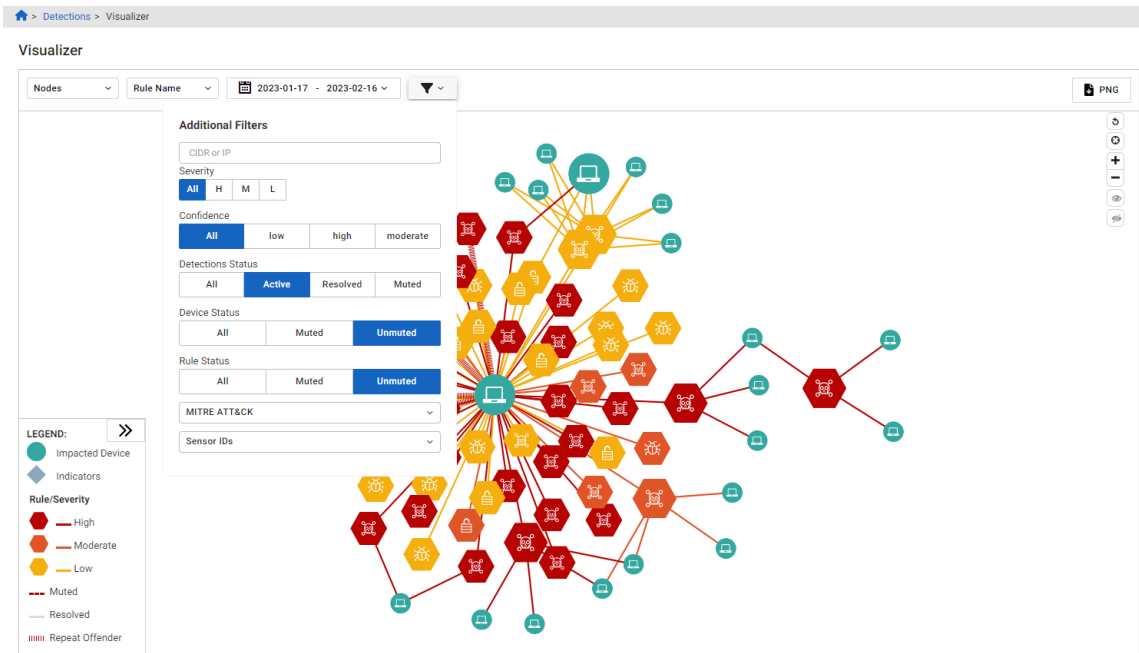
## Date Range

Use the date-range selector to specify the date range to display.



## Filter by Status

You can refine the results in the Visualizer by *Detection Status*, *Device Status*, or *Rule Status*. Changing the status filters will initiate a new query to the Detections API and refresh the graph. All other filter changes will filter the existing data and redraw the graph.

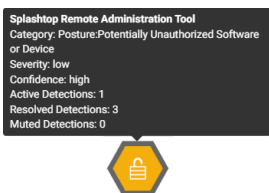


## Nodes

You can hover over all the nodes in the Visualizer to view summary information about a rule, device, indicator or connector line. Click a node to open the *Quick View* panel on the right side of the page. Right-click a node to open a context menu.

### Rule nodes

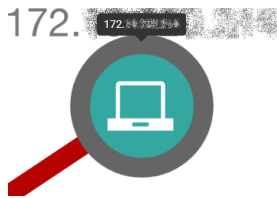
Hover over a rule node to view related information about the detection such as the rule's *Category*, *Severity*, *Confidence* rating as well as the number of *Active* and *Resolved Detections*. The rule and its impacted devices are also highlighted.



## Device nodes

Hover over a device node, to view the device IP address. If you hover over a device group, the list of IP addresses is shown. The device group and related rules will be highlighted.

Right-click a device node to show/hide the label or the node, add an annotation, or mute the device



## Indicator node

Hover over an indicator node to view the indicator and to highlight related rules and devices.

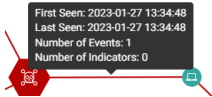
Right-click an Indicator node to show/hide the label or the node, or add an annotation.



## Connector lines

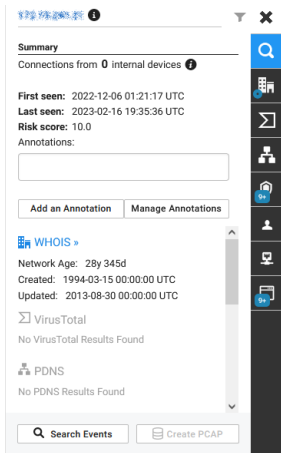
Hover over the connector lines to view summary information pertaining to what the line connects, such as the indicators, device IPs, and/or rules. Related devices, rules, or indicators will be highlighted.

Right-click a connector line to resolve the detection or mute the device for that rule. If any node is a group or can be grouped, you will have an option to *Expand* (ungroup) or *Collapse* (regroup) the set of nodes.



## Quick views

Click a node in the Visualizer to open the *Quick View* panel at the right side of the screen. Quick Views display summary information as well as a series of detail-view options and actions. The available options and actions will vary depending on the type of node selected.



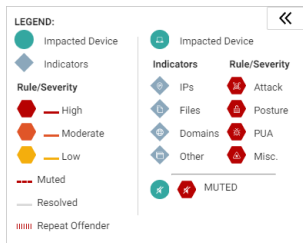
|  |                    |  |
|--|--------------------|--|
|  | <b>Summary</b>     | Provides a summary of the detection and corresponding devices along with options to access further details:  |
|  | <b>Software</b>    | Displays the <i>Version</i> , <i>Events</i> , <i>First Seen</i> and <i>Last Seen</i> for the software detected on the device.  |
|  | <b>Indicators</b>  | Displays the Indicators list.  |
|  | <b>Accounts</b>    | Displays the Account, User, First Seen, Last Seen and Service detected on the device.  |
|  | <b>DHCP</b>        | Displays the Dynamic Host Configuration Protocol.  |
|  | <b>Detections</b>  | Shows a list of detections, each citing the date and time it was last seen and the impacted account; <ul style="list-style-type: none"> <li>• Click an item to open the Rule view</li> <li>• Click the options drop-down on an item to resolve the detection or mute the device for the specified rule or account</li> </ul> |
|  | <b>PDNS</b>        | Displays the Passive DNS/  |
|  | <b>Signature</b>   | Displays the signatures.   |
|  | <b>Virus Total</b> | Displays the total number of viruses detected.   |
|  | <b>WHOIS</b>       | Provides registered domain information.  |

## Visualizer controls

You can use your mouse to zoom in and out of the canvas. Each node in the graph can be dragged to a new location.

## Graphics legend

The legend provides details about the specific devices, indicators, and rules.



### Shapes

- Shape represent the type of node.
- Color is used for severity of rules.
- Size is used for nodes representing multiple detections.
- Icons in the node show the type of indicator or rule.

### Lines

- Dashed edges indicate muted detections.
- Thick, dotted lines indicate *repeat offender* detections (active detections that have occurred previously).
- Solid, colored lines indicate active detections (with the color matching the severity of the rule).
- Grey lines are used for other linkages.

## Action buttons

|  |   |
|--|---|
|  | Export the current graph as a PNG file.   |
|  | Reset the graph (resets all filters, reloads data, and generates a new graph).  |
|  | Recenter the graph (fits all existing data in the screen).  |
|  | Zoom in or out.   |
|  | Reveal hidden nodes. This option is available after one or more nodes have been hidden. To hide a node, right-click it and select <i>Hide node</i> .  |
|  | Hide hidden nodes. This option is available after one or more nodes have been hidden. to hide a node, right-click on it, and click <i>Hide node</i> . |

## Detections Table

The *Detections Table* is where you can view all detections. Whereas the *Triage Rule* and *Detections Triage* views show detections by rule or device, the *Detections Table* shows detections by rule and device over time. By default, the table displays detections for the last two weeks. A color-coded bar at the left side of the table indicates active and resolved detections. A green bar indicates an active detection. A red bar indicates a resolved detection.

### To access the Detections Table:

- Go to *Detections > Detections Table*.
- On the *Dashboard*:
  - In the *MITRE ATT&CK* widget, click a bar in the chart.
  - In the *Resolved Detections* widget, click *Total* or click a data point in the chart.

Detection List 14 Detection Rules, 1361 Devices from 5000 Detections (out of 6818 total Detections)

Device IP to search  Search 2023-06-09 - 2023-06-23 Severity **All** H M L Detection Status **All** Active Resolved ▼ □ ↓ CSV 📄 ⌂ ⚙

| <input type="checkbox"/> | Detection UUID               | Device IP | DHCP Ho... | Username | Hostname | MAC Address | Lifetime Events | Action |
|--------------------------|------------------------------|-----------|------------|----------|----------|-------------|-----------------|--------|
| <input type="checkbox"/> | cfeba5b8-cf13-42fb-80aa-e... | ...       |            |          |          |             | 40 Events       | ⋮      |
| <input type="checkbox"/> | d6637bd5-0299-4398-a4b8-...  | ...       |            |          |          |             | 6 Events        | ⋮      |
| <input type="checkbox"/> | 2849c0a8-f3bf-445b-a458-6... | ...       |            |          |          |             | 1 Event         | ⋮      |
| <input type="checkbox"/> | 7809918b-0b25-47f5-a987-...  | ...       |            |          |          |             | 1 Event         | ⋮      |

## Filtering events

By default, the *Detections Table* displays detections by all severities and detection statuses for the previous two weeks ending on the current date. Filters allow you to view detections for a specific IP, refine the list by *Severity* and *Detection Status*. You can also toggle between table and graph view.

Detection List 2 Detection Rules, 1 Devices from 2 Detections

Device IP to search  Search 2023-06-06 - 2023-06-20 Severity **All** H M L Detection Status **All** Active Resolved ▼ □ ↓ CSV 📄 ⌂ ⚙

| <input type="checkbox"/> | Detection UUID              | Device IP     | DHCP Ho... | Username | Hostname | MAC Address | Lifetime Events | Action |
|--------------------------|-----------------------------|---------------|------------|----------|----------|-------------|-----------------|--------|
| <input type="checkbox"/> | 576c04a2-10d5-42bf-bc94-... | 10.10.150.112 |            |          |          |             | 1 Event         | ⋮      |
| <input type="checkbox"/> | b287c345-ace7-4d8d-b9dc-... | 10.10.150.112 |            |          |          |             | 1 Event         | ⋮      |

|          |                            |  |
|----------|----------------------------|--|
| <b>1</b> | <b>Device IP to search</b> | Enter the IP of a specific device.   |
| <b>2</b> | <b>Time range</b>          | Click to open the date picker.<br>Use the calendar to set the start and end date or select an option from the <i>Quick Ranges</i> ( <i>Last Hour</i> to <i>Last 90 days</i> ).<br>Click <i>Resolution Date</i> to show all detections resolved within the time range. This will disable the buttons in the <i>Severity</i> area. |
| <b>3</b> | <b>Severity</b>            | Select High (H), Medium (M), or Low (L).   |

|                 |                                  |   |
|-----------------|----------------------------------|---|
| <p><b>4</b></p> | <p><b>Detection Status</b></p>   | <p><b>All</b> Detections that were active during time range and are still active or resolved now.<br/>For example, a detection that was active on May 5 and resolved on May 10 is counted as <i>ALL</i>.</p> <p><b>Active</b> Detections that were active during time range and are still active.</p> <p><b>Resolved</b> Detections that were active during time range and are resolved now.</p>  |
| <p><b>5</b></p> | <p><b>Additional filters</b></p> | <p><b>Category</b> Select a category from the list. See, Detections &gt; <a href="#">Rule Categories on page 61</a>.</p> <p><b>Created By</b> Select and account from the list.</p> <p><b>MITRE ATT&amp;CK</b> Select the detection by behavior from the list. See, <a href="#">MITRE ATT&amp;CK on page 54</a>.</p> <p><b>Resolved by</b> Select a user from the list.</p> <p><b>Resolution</b> Select <i>All, True Positive: Mitigated, True Positive: No Action, False Positive, or Unknown</i>.</p> <p><b>Sensor</b> Select a sensor from the list.</p> <p><b>Rule Name</b> Select a parameter used for the detection from the list.</p> <p><b>Confidence</b> Select <i>All, High (H), Medium (M), or Low (L)</i>.</p> <p><b>Muted</b> Select <i>All, Unmuted or Muted</i>. See, <a href="#">Muting rules on page 66</a>.</p> <p><b>Disabled</b> Select <i>All, Enabled or Disabled</i>. See, <a href="#">Disabling rules on page 69</a>.</p> |
| <p><b>6</b></p> | <p><b>Columns selectors</b></p>  | <p><b>Individual Columns</b> Select one of the following options:</p> <ul style="list-style-type: none"> <li>• Show all columns</li> <li>• Hide All Columns</li> <li>• Reset to default</li> <li>• Select columns to show or hide in the table.</li> </ul>  |

**Column Profiles**

Select one of the following options:

- Click a profile in the list to view the layout.
- Save the profile
- Create a new profile.

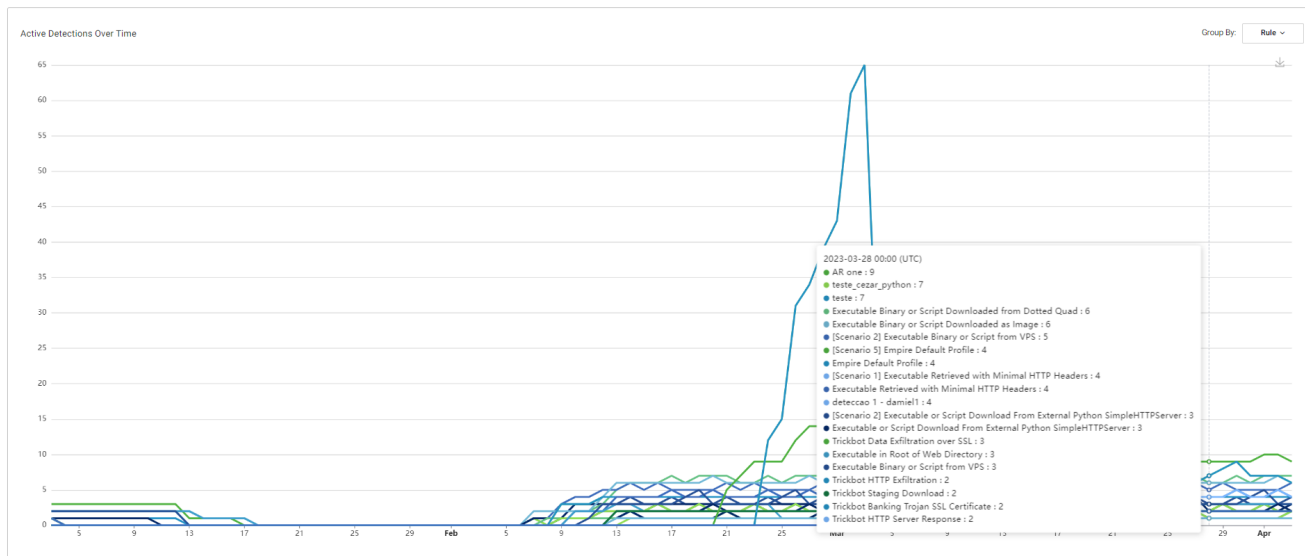
For more information, see [Creating column profiles on page 90](#)

|    |              |  |
|----|--------------|--|
| 7  | CSV          | Click to export the list as a CSV file.  |
| 8  | Table View   | Click for table view (default).  |
| 9  | Graph View   | Click to open the Visualizer.  |
| 10 | Actions menu | Select one of the following options: <ul style="list-style-type: none"> <li>• Create Rules</li> <li>• Manage Rules</li> <li>• Muted Devices</li> <li>• Excluded devices</li> <li>• Manage Subscriptions</li> </ul> |

## Statistics

The *Statistics* page shows the *Active Detections Over Time* graph. Hover a line in the graph to view the defections for specific day. You can group the statistics by *Rule*, *Category* or *Severity*.

Detections Statistics





# Manage My Rules

The *Manage My Rules* page allows you to view, edit and create rules. You can also mute, disable and delete rules.

| Rule                             | Severity | Confidence | Devices | Owner | Category                   | Rule Updated           | Actions |
|----------------------------------|----------|------------|---------|-------|----------------------------|------------------------|---------|
| REvil Drive-by compromises       | HIGH     | HIGH       | 0       |       | Attack-Infection Vector    | 2023-11-30 23:24 (UTC) |         |
| dhcp                             | HIGH     | HIGH       | 0       |       | Attack-Infection Vector    | 2023-12-01 18:08 (UTC) |         |
| PetitPotam Forced Authentication | HIGH     | HIGH       | 0       |       | Attack-Exploitation        | 2023-12-08 23:16 (UTC) |         |
| AR T1595                         | HIGH     | MOD        | 0       |       | Attack-Infection Vector    | 2023-09-07 22:48 (UTC) |         |
| ⊗ [Rule Name]                    | HIGH     | HIGH       | 0       |       | Attack-Infection Vector    | 2023-12-08 00:11 (UTC) |         |
| ⊗ [Rule Name]                    | HIGH     | MOD        | 0       |       | Attack-Infection Vector    | 2023-11-28 17:26 (UTC) |         |
| ⊗ [Rule Name]                    | HIGH     | MOD        | 0       |       | Attack-Exploitation        | 2023-03-16 22:34 (UTC) |         |
| ⊗ [Rule Name]                    | HIGH     | MOD        | 0       |       | Attack-Infection Vector    | 2023-12-07 23:31 (UTC) |         |
| [Rule Name]                      | HIGH     | HIGH       | 0       |       | Attack-Infection Vector    | 2022-06-10 20:08 (UTC) |         |
| Exploit Kit                      | HIGH     | MOD        | 0       |       | Attack-Exploitation        | 2022-07-21 18:18 (UTC) |         |
| [Rule Name]                      | HIGH     | MOD        | 0       |       | Attack-Infection Vector    | 2021-10-14 17:49 (UTC) |         |
| ⊗ AR 1                           | MOD      | HIGH       | 0       |       | Attack-Infection Vector    | 2021-10-03 07:48 (UTC) |         |
| [Rule Name]                      | MOD      | MOD        | 15      |       | Posture-Anomalous Activity | 2023-12-08 15:54 (UTC) |         |
| ⊗ New rule from investigation    | MOD      | MOD        | 0       |       | Attack-Exploitation        | 2022-01-06 00:14 (UTC) |         |
| ⊗ AR PDST                        | MOD      | MOD        | 0       |       | Attack-Infection Vector    | 2021-10-25 06:39 (UTC) |         |
| AR twos                          | MOD      | HIGH       | 0       |       | Attack-Infection Vector    | 2023-11-30 20:01 (UTC) |         |
| [Rule Name]                      | MOD      | MOD        | 0       |       | Attack-Installation        | 2023-11-30 23:20 (UTC) |         |

The Manage my Rules page displays the following information:

|                      |   |
|----------------------|---|
| <b>Rule</b>          | Click to view the rule details. An icon is displayed with the rule is disabled (⊗) or muted (⊗).  |
| <b>Muted</b>         | Displays an icon that indicates the rule is muted (⊗) or unmuted (⊗).   |
| <b>Enabled</b>       | Displays an icon that indicates the rule is enabled (⊗) or disabled (⊗).  |
| <b>Severity</b>      | The FortiGuard ATR severity level (Low, Moderate or High).  |
| <b>Confidence</b>    | The FortiGuard ATR confidence level (Low, Moderate or High).  |
| <b>Devices</b>       | The number of devices impacted by the rule. To view the devices, click the link in the <i>Rules</i> column and review the details in the <i>Impacted Devices</i> and <i>Events</i> tab. |
| <b>Muted Devices</b> | The number of devices muted for the rule.   |
| <b>First</b>         | The date the rule was first detected.   |
| <b>Last</b>          | The date the rule was last detected.  |
| <b>Owner</b>         | The account name.   |
| <b>Category</b>      | The rule category.  |
| <b>Rule updated</b>  | The date the rule was updated.  |
| <b>Actions</b>       | Click the dropdown menu to: <ul style="list-style-type: none"> <li>• Edit</li> <li>• Mute Rule</li> </ul>   |

- Mute Device for Rule
- Enable Rule
- Delete Rule

The following tools are available in the toolbar

| <input type="text" value="Search titles"/> | Filter the table by the rule name.  |        |             |                 |   |                  |  |                   |  |                         |  |              |  |                 |   |
|--|---|--------|-------------|-----------------|---|------------------|--|-------------------|--|-------------------------|--|--------------|--|-----------------|---|
| Severity <b>All</b> H M L                  | Filter the table by the FortiGuard ATR confidence level (Low, Moderate or High).  |        |             |                 |   |                  |  |                   |  |                         |  |              |  |                 |   |
|  | Additional filters. Filters persist until you refresh the page (except for <i>Search title</i> ). An indicator (●) is added when you change a filter from the default. A number indicates the number of changes that were applied. Click <i>Reset to Default</i> to clear the filters.  |        |             |                 |   |                  |  |                   |  |                         |  |              |  |                 |   |
|  | <table border="1"> <thead> <tr> <th>Filter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>Category</b></td> <td>Click to select a category from the dropdown.</td> </tr> <tr> <td><b>Technique</b></td> <td>Click to select a technique from the dropdown.</td> </tr> <tr> <td><b>Confidence</b></td> <td>Filter by FortiGuard ATR confidence level (All, H, M or H). <i>All</i> is the default.</td> </tr> <tr> <td><b>Detection Status</b></td> <td>Filter by detection status (<i>All</i>, <i>Active</i> or <i>Idle</i>). <i>All</i> is the default.</td> </tr> <tr> <td><b>Muted</b></td> <td>Select <i>Unmuted</i> or <i>Muted</i> . <i>All</i> is the default.</td> </tr> <tr> <td><b>Disabled</b></td> <td>Select <i>Enabled</i> or <i>Disabled</i>. <i>All</i> is the default.</td> </tr> </tbody> </table> | Filter | Description | <b>Category</b> | Click to select a category from the dropdown. | <b>Technique</b> | Click to select a technique from the dropdown. | <b>Confidence</b> | Filter by FortiGuard ATR confidence level (All, H, M or H). <i>All</i> is the default. | <b>Detection Status</b> | Filter by detection status ( <i>All</i> , <i>Active</i> or <i>Idle</i> ). <i>All</i> is the default. | <b>Muted</b> | Select <i>Unmuted</i> or <i>Muted</i> . <i>All</i> is the default. | <b>Disabled</b> | Select <i>Enabled</i> or <i>Disabled</i> . <i>All</i> is the default. |
| Filter                                     | Description   |        |             |                 |   |                  |  |                   |  |                         |  |              |  |                 |   |
| <b>Category</b>                            | Click to select a category from the dropdown.   |        |             |                 |   |                  |  |                   |  |                         |  |              |  |                 |   |
| <b>Technique</b>                           | Click to select a technique from the dropdown.  |        |             |                 |   |                  |  |                   |  |                         |  |              |  |                 |   |
| <b>Confidence</b>                          | Filter by FortiGuard ATR confidence level (All, H, M or H). <i>All</i> is the default.  |        |             |                 |   |                  |  |                   |  |                         |  |              |  |                 |   |
| <b>Detection Status</b>                    | Filter by detection status ( <i>All</i> , <i>Active</i> or <i>Idle</i> ). <i>All</i> is the default.  |        |             |                 |   |                  |  |                   |  |                         |  |              |  |                 |   |
| <b>Muted</b>                               | Select <i>Unmuted</i> or <i>Muted</i> . <i>All</i> is the default.  |        |             |                 |   |                  |  |                   |  |                         |  |              |  |                 |   |
| <b>Disabled</b>                            | Select <i>Enabled</i> or <i>Disabled</i> . <i>All</i> is the default.   |        |             |                 |   |                  |  |                   |  |                         |  |              |  |                 |   |
|  | Show or hide all columns in the table, or select the columns you want to view.  |        |             |                 |   |                  |  |                   |  |                         |  |              |  |                 |   |
|  | Set the page height.  |        |             |                 |   |                  |  |                   |  |                         |  |              |  |                 |   |
|  | Create a new rule. See <a href="#">Creating a rule on page 71</a> .   |        |             |                 |   |                  |  |                   |  |                         |  |              |  |                 |   |

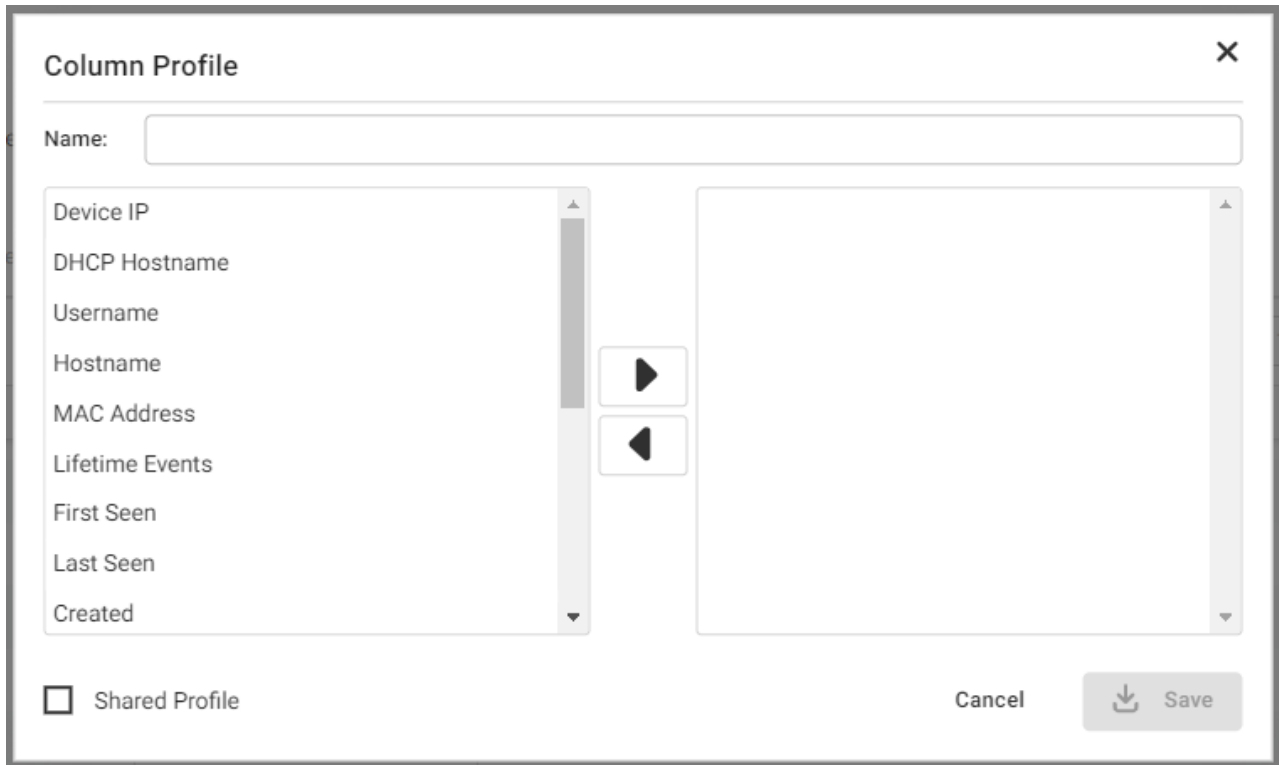
## Creating column profiles

Custom column profiles can be created for any table that allows columns to be selected. When selecting the individual columns or column profile for a table, they are organized into groups. Custom profiles can be shared with other users in your organization.

### To create a column profile:

1. Click the column selector icon.
  -
2. Create the profile by clicking:
  - *New profile*
  - *Save this profile*

3. In the *Column Profile* dialog, enter a *Name* for the profile and then use the arrows to select the column headings to display.



4. (Optional) Click *Shared* to share the column profile with other members of your organization.
5. Click *Save*.

# Investigations

Use the tools in the *Investigations* module to respond to detections and to hunt for malicious activity on your network.

## Entity Lookup

An *Entity Lookup* (or search) is the starting point for an investigation if you have very little information to work with, because the entity record may contain important contextual information.

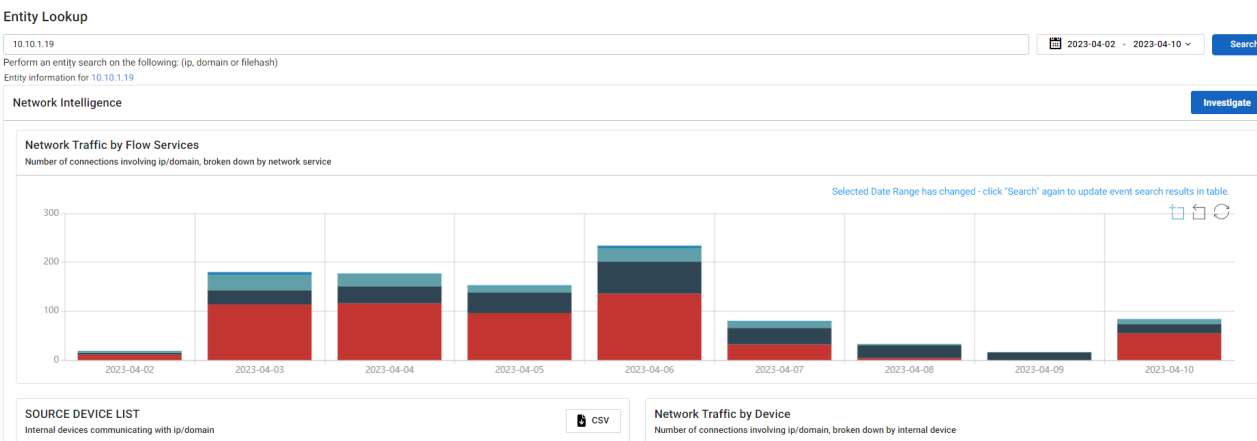


You can start an Entity Search by entering an IP address or domain in the *Search* field in the navigation menu at the top of the portal.

### To perform an entity lookup:

1. Go to *Investigations > Entity Lookup*.
2. Enter an IP address or a domain name in the search field. Separate Multiple IP addresses and domain names by spaces.
3. Click the date picker to select the time range. The default is *Last Seven Days*. The maximum is 90 days.
4. Click *Search*. The following results are returned.

|                              |   |
|------------------------------|---|
| <b>Network Intelligence</b>  | Network traffic by service, by device, and source addresses interacting with the entity |
| <b>Entity Intelligence</b>   | WHOIS, IP History, Registrar History, Passive DNS                                       |
| <b>Security Intelligence</b> | Associated VirusTotal Detections and VirusTotal Detections Over Time                    |





You can view the *Entity Panel* by clicking the IP address at the top-left of the page next to *Entity information for <IP address>*.

5. (Optional) If multiple IP addresses or domain names are looked up, right-click on a result and select *Entity Lookup* to view the intelligence panes.
6. (Optional) Click *Investigate* to launch the new investigation.

**To perform a bulk entity export:**

1. In the search field, enter IP addresses or a domain names separated by spaces.
2. Click *Search*.
3. Click the CSV button. A CSV file with the *timestamp*, *action*, *param*, *user\_uuid*, *account\_uuid*, and *account* are downloaded to your device.

Investigations > Entity Lookup

Entity Lookup

10.10.1.19 10.10.1.17 2023-03-31 - 2023-04-10 Search

Perform an entity search on the following: (ip, domain or filehash)

2 Results CSV

| Entity     | Type | Count | First Seen             | Last Seen              |
|------------|------|-------|------------------------|------------------------|
| 10.10.1.17 | IP   | 0     | 2022-06-06 04:17 (UTC) | 2023-03-30 20:08 (UTC) |
| 10.10.1.19 | IP   | 869   | 2022-05-11 16:52 (UTC) | 2023-04-10 21:09 (UTC) |

## Source Device List

View the internal devices communicating with the specific IP or domain. Right-click the IP address of any source device and click *Investigate*.

SOURCE DEVICE LIST CSV

Internal devices communicating with ip/domain

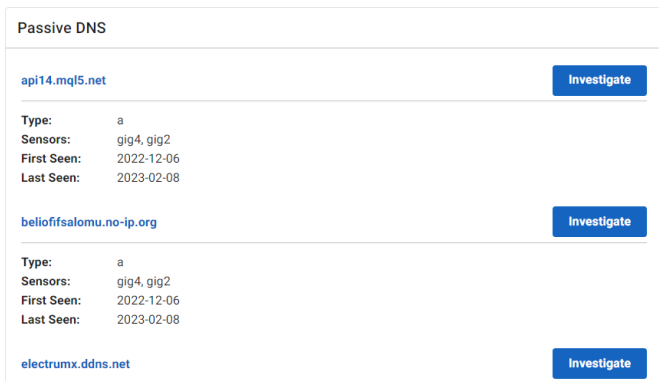
| Device  | Event Count | PDNS                               |
|---------|-------------|------------------------------------|
| 0.0.0.0 | 8           | 1jadedcolossal.pointto.us, alos... |

Context menu for 0.0.0.0:

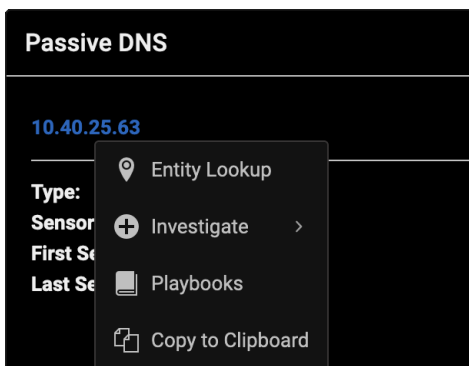
- Entity Lookup
- Investigate
- Playbooks
- Copy to Clipboard

## Passive DNS

Passive DNS links on the entity panel function like normal links. Clicking the link replaces the entity panel with the panel for the clicked on element.



Right-clicking opens a context menu.



| Option                   | Description  |
|--------------------------|--|
| <b>Entity Lookup</b>     | Open the entity lookup page for the item.  |
| <b>Copy to Clipboard</b> | Copy the item to the clipboard.  |
| <b>Playbooks</b>         | Launch playbooks. This options is not available for ad-hoc search result items   |
| <b>Investigate</b>       | Show appropriate pivots for the item type. This options is not available for ad-hoc search result items.   |
| <b>Search Events</b>     | Show the event searches appropriate for the type. The text in the search box is replaced, but the search will not run automatically. This options is only available for ad-hoc search result items.<br>Types include: <ul style="list-style-type: none"> <li>• IP:                             <ul style="list-style-type: none"> <li>• ip='IP'</li> <li>• dst.ip='IP'</li> <li>• src.ip='IP'</li> </ul> </li> <li>• domain:                             <ul style="list-style-type: none"> <li>• domain='domain'</li> </ul> </li> </ul> |

# Investigate

Investigations allow you to quickly obtain details required in investigations via search queries and/or playbooks.

| Name  | Description | Created by | Date Created           | Date Updated           | Activities | Queries |
|---|-------------|------------|------------------------|------------------------|------------|---------|
| adhoc tag                                     |             |            | 2023-06-13 22:02 (UTC) | 2023-07-18 18:17 (UTC) |            | 8       |
| Test For Tagging                              | (Closed)    |            | 2023-06-05 22:11 (UTC) | 2023-06-21 16:13 (UTC) |            | 13      |
| 2023-05-30 16:50:21 (UTC)                     |             |            | 2023-05-30 16:50 (UTC) | 2023-06-16 18:41 (UTC) |            | 2       |
| 2023-04-13 16:50:43 (UTC)                     |             |            | 2023-04-13 16:50 (UTC) | 2023-06-19 22:48 (UTC) |            | 34      |
| 2023-02-21 22:33:43 (UTC)                     |             |            | 2023-02-21 22:33 (UTC) | 2023-05-25 16:41 (UTC) |            | 6       |
| j5yZb8stFT9KxH4L0eEz6ZUcQ1wV7mXhYpPnDIAaRq3vS |             |            | 2022-09-24 00:38 (UTC) | 2023-06-19 22:12 (UTC) |            | 92      |
| APT23   | (Closed)    |            | 2022-06-15 19:26 (UTC) | 2023-06-21 17:11 (UTC) |            | 91      |

The Investigations page displays the following information:

|                     |   |
|---------------------|---|
| <b>Name</b>         | The investigation name.                           |
| <b>Description</b>  | The description of the investigation.             |
| <b>Created by</b>   | The user who created the investigation.           |
| <b>Date Created</b> | The date the investigation was created.           |
| <b>Date Updated</b> | The date the investigation was updated.           |
| <b>Queries</b>      | The number of queries added to the investigation. |

Click the filter icon next to the Search field to view by:

- All: Open and closed investigations
- Open: Only the open investigations
- Closed: Only the closed investigations
- Related detections

| Name  | Description | Created by | Date Created           | Date Updated           | Activities | Queries |
|---|-------------|------------|------------------------|------------------------|------------|---------|
| adhoc tag                                     |             |            | 2023-06-13 22:0        |                        |            | 8       |
| Test For Tagging                              | (Closed)    |            | 2023-06-05 22:1        |                        |            | 13      |
| 2023-05-30 16:50:21 (UTC)                     |             |            | 2023-05-30 16:5        |                        |            | 2       |
| 2023-04-13 16:50:43 (UTC)                     |             |            | 2023-04-13 16:5        |                        |            | 34      |
| 2023-02-21 22:33:43 (UTC)                     |             |            | 2023-02-21 22:33 (UTC) | 2023-05-25 16:41 (UTC) |            | 6       |
| j5yZb8stFT9KxH4L0eEz6ZUcQ1wV7mXhYpPnDIAaRq3vS |             |            | 2022-09-24 00:38 (UTC) | 2023-06-19 22:12 (UTC) |            | 92      |
| APT23   | (Closed)    |            | 2022-06-15 19:26 (UTC) | 2023-06-21 17:11 (UTC) |            | 91      |



The selected filters are persistent. For example, if you sort the table by *Date Updated* and then browse to a different page in the GUI, the investigations table will still be sorted by *Date Updated* when you return to the Investigations page.

When you add filters, the filter chips will be shown under search bar.



## Creating investigations

An investigation is run against the account shown in the account picker. The account name that owns the investigation appears to the right of the investigation name if it differs from your primary account.



- If you have access to multiple accounts and the account shown in the account picker is different from the account that contains your user, then the account is listed.
- If you have access to multiple accounts, and the account shown in the account picker is the same as the account that contains your user, then the account is not shown in the investigation list. The investigation created is run against the account shown in the account picker.

### To create an investigation:

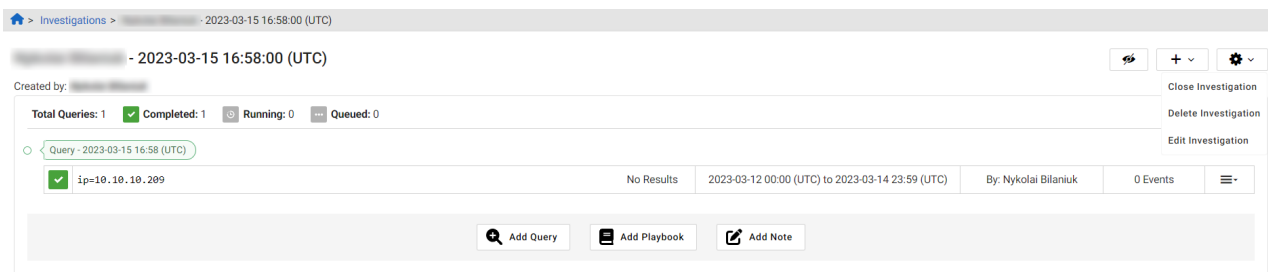
1. Go to *Investigations* and click *New Investigation* at the top-right corner of the page. The *New Investigation* dialog opens.

The default investigation name is the first and last name of the user creating the investigation with the time stamp of when the investigation was created.

2. Enter an *Investigation name* and *Description*, then click *Create Investigation*.
3. Add the following to your investigation:
  - Query: [Adding queries to an investigation on page 99](#)
  - Playbook: [Adding a playbook to an investigation on page 127](#)
  - Notes: [Adding notes to an investigation on page 101](#)

### To close an investigation:

1. Go to *Investigations* and click the investigation you want to close.
2. Click the gear icon at the top-right side of the page and select *Close Investigation*. A confirmation dialog opens.



3. Click *Close Investigation*.



**To delete an investigation:**

1. Go to *Investigations* and click the investigation you want to delete.
2. Click the gear icon at the top-right side of the page and select *Delete Investigation*. A confirmation dialog opens.
3. Click *Confirm*.



Deleting an investigation is irreversible and will remove everything in the investigation

**To edit an investigation name:**

1. Go to *Investigations* and click the investigation you want to edit.
2. Click the gear icon at the top-right side of the page and select *Edit Investigation*. A dialog opens.
3. Update the *Investigation name* and *Description* and click *Save*.

## Viewing investigation details

**To view the investigation details.**

1. Go to *Investigations*, and click an investigation name.
2. Click an investigation name. The investigations details page displays the following information:
  - Investigation Creator
  - Link to single or multiple related detections
  - IQL query
  - Notes (if any)
  - Date/time the query was added
  - Number of events (if complete)
  - Executed Playbooks that are part of that investigation
  - Close date (if investigation was closed)

Investigation from detection rule AR low cat rule

Created by: [John Doe](#)  
Related Detection Rule: [AR low cat rule](#)

Total Queries: 1 ✔ Completed: 1 ⏸ Running: 0 ⏸ Queued: 0

Query: Query from detection rule AR low cat rule - 2022-03-18 05:22 (UTC)

✔ ip = "10.0.0.1" View Results 2022-03-11 05:19 (UTC) to 2022-03-18 05:18 (UTC) By: [John Doe](#) 100 Events ☰

Add Query Add Playbook Add Note



If the investigation contains more than one related detection, the *MORE>>* link appears. You can click the link to view all the related detections.

## Query Status Icons



Query completed successfully. Results (if any) are available.



Query is currently running.



Query is queued to run. It will run automatically when resources are available.



Query failed due to an internal error. If problem persists, please contact Fortinet support.

You can click any related detections name to view detection details.

The screenshot displays the 'cross 2' investigation page. A modal window titled 'Related Detection Rules' is open, showing two rules: 'pretend detection' and 'AR low cat rule'. The background interface shows a list of queries with their status (Completed, Running, Queued) and a table of events. The table has columns for time, user, and event count. At the bottom, there are buttons for 'Add Query', 'Add Playbook', and 'Add Note'.

## View results

Click the *View Results* to view the following information:

- IQL Query string
- Date Range
- Number of events
- A table of the events where you can:
  - Click on column filter to change the visible columns in the way that the current event search does including column visibility sets.
  - Click the CSV button to export the results as a CSV file



Hold down the Shift key and use the scroll wheel on your mouse to quickly scroll through the column headings.

Investigation Results | New investigation 03162022-1 | Query from investigation results

```
(dns:query.domain = "google.com")
/* include filters */
and ((answers.ip = "8.8.8.8"))
/* exclude filters */
exclude (dst.in = "8.8.8.8")
```

FILTERS: answers.ip • Includes: [8.8.8.8] • dst.ip • Excludes: [8.8.8.8] [Clear All] [Create New Query]

Events grouped by src.ip and day(timestamp) **Events**

Showing first 29 events, sorted by timestamp descending *Facets were requested, but none were available with the results.* [CSV]

| timestamp             | type | src | dst | intel        | proto | source | query | answers    | applicat |
|-----------------------|------|-----|-----|--------------|-------|--------|-------|------------|----------|
| 2022-03-11 22:11:22 Z | DNS  | ... | ... | 2 Annotation | 1 Hit | udp    | Zeek  | google.com | ...      |
| 2022-03-11 21:11:22 Z | DNS  | ... | ... | 2 Annotation | 1 Hit | udp    | Zeek  | google.com | ...      |
| 2022-03-11 20:11:22 Z | DNS  | ... | ... | 2 Annotation | 1 Hit | udp    | Zeek  | google.com | ...      |
| 2022-03-11 19:11:21 Z | DNS  | ... | ... | 2 Annotation | 1 Hit | udp    | Zeek  | google.com | ...      |
| 2022-03-11 18:11:22 Z | DNS  | ... | ... | 2 Annotation | 1 Hit | udp    | Zeek  | google.com | ...      |
| 2022-03-11 17:11:22 Z | DNS  | ... | ... | 2 Annotation | 1 Hit | udp    | Zeek  | google.com | ...      |
| 2022-03-11 16:11:22 Z | DNS  | ... | ... | 2 Annotation | 1 Hit | udp    | Zeek  | google.com | ...      |
| 2022-03-11 15:11:22 Z | DNS  | ... | ... | 2 Annotation | 1 Hit | udp    | Zeek  | google.com | ...      |
| 2022-03-11 14:11:21 Z | DNS  | ... | ... | 2 Annotation | 1 Hit | udp    | Zeek  | google.com | ...      |
| 2022-03-11 13:11:22 Z | DNS  | ... | ... | 2 Annotation | 1 Hit | udp    | Zeek  | google.com | ...      |
| 2022-03-11 12:11:21 Z | DNS  | ... | ... | 2 Annotation | 1 Hit | udp    | Zeek  | google.com | ...      |
| 2022-03-11 11:11:21 Z | DNS  | ... | ... | 2 Annotation | 1 Hit | udp    | Zeek  | google.com | ...      |

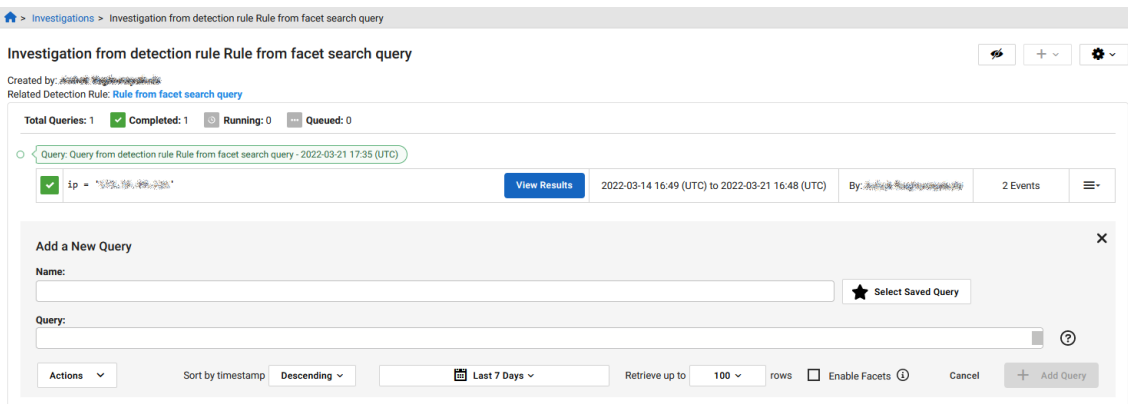
## Adding queries to an investigation

You can add one or more queries to an investigation.

### To add a query to an investigation:

1. Go to *Investigations* and click an investigation the list.
2. Click *Add Query*. The *Add a New Query* page opens.
3. Configure the query settings.

|                                |   |
|--------------------------------|---|
| <b>Name</b>                    | Enter a name for the query.   |
| <b>Select Saved Query</b>      | Click to base the new query on a saved query.   |
| <b>Query</b>                   | Enter the query string.   |
| <b>Actions</b>                 | Options are: <ul style="list-style-type: none"> <li>• <i>Bulk Add Indicators</i></li> <li>• <i>Create a Detection</i></li> </ul>  |
| <b>Sort by timestamp</b>       | Select <i>Ascending</i> or <i>Descending</i> .  |
| <b>Last 7 Days</b>             | Use the date picker to update the date range and click <i>Apply</i> .   |
| <b>Retrieve up to xxx rows</b> | Select between 100 to 10,000 rows.  |
| <b>Enable Facets</b>           | Select to return the panel that allows narrowing the search. This may make the query longer to complete. For more information, see <a href="#">Facet Search on page 103</a> . |



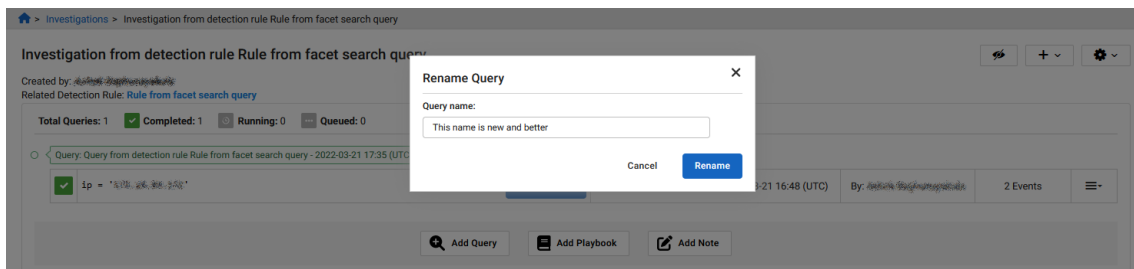
4. Click *Add Query*.
5. (Optional) To add another query to the investigation, click *Add Query*.

**To rename a query:**

1. From the Investigation Detail page, locate the query you want to rename.
2. Click the *Actions* menu on the right side of the page and select *Rename*.



3. Enter the name in the *Query name* field.



4. Click *Rename*.

**To clone a query:**



You can clone a query in a closed investigation. However, the cloned query must be added to a different investigation.

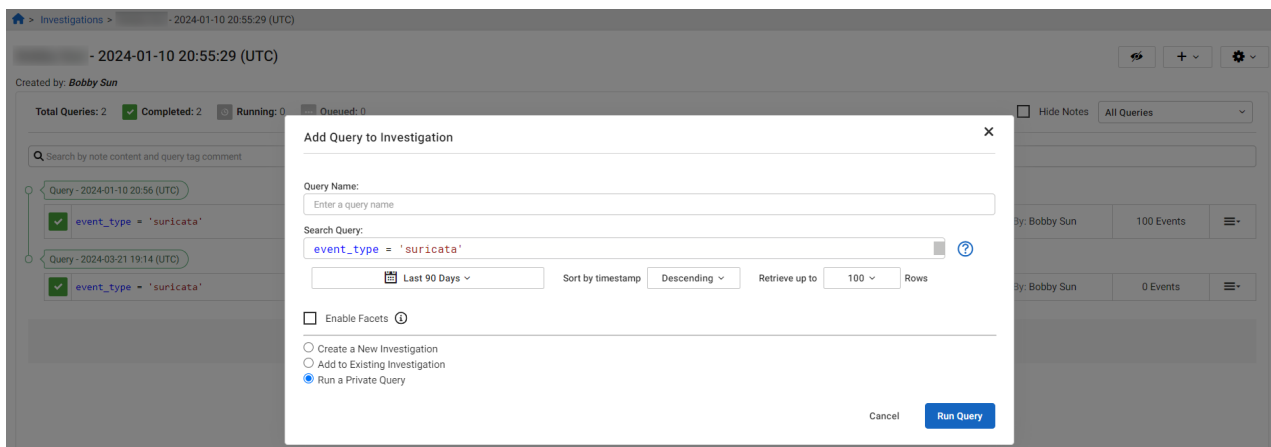
1. Click *Investigations*.
2. Click the investigation that contains the query you want to clone.
3. Click the *Actions* menu on the right side of the page and select *Clone*. The *Add Query to Investigation* dialog opens.
4. Configure the query settings.
5. Create a new investigation or save the query to an existing investigation.

**Create a New Investigation**

Enter an *Investigation Name* and *Description*.

**Add to Existing Investigation** From the *Choose Investigation* dropdown, select an investigation. By default the cloned query is added to current investigation.

**Run a Private Query** Select this option to add a query to an adhoc search.



6. Click *Add Query*.

### To delete a query:

1. Click *Investigations*.
2. Click the investigation that contains the query you want to delete.
3. Click the *Actions* menu on the right side of the page and select *Delete*. The *Delete Query* dialog opens.
4. Click *Confirm*.

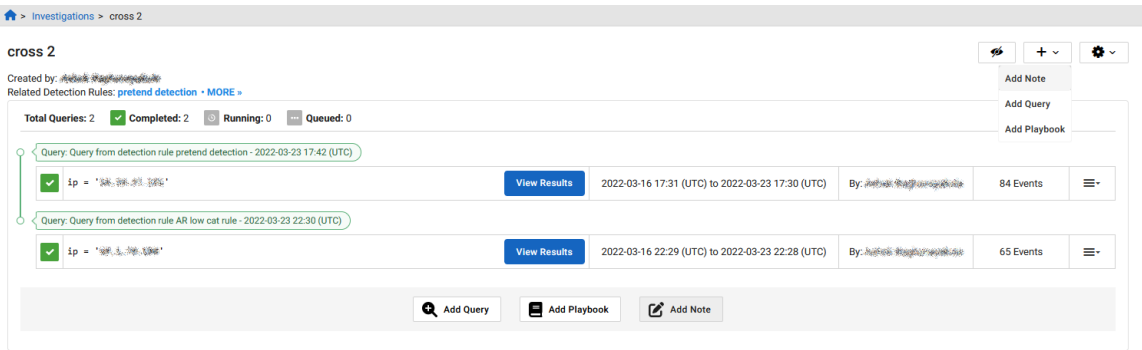
### To save a query:

1. Click *Investigations*.
2. Click the investigation that contains the query you want to save.
3. Click the *Actions* menu on the right side of the page and select *Save*. The *Save Query* dialog opens.
4. Enter a *Query Name* and *Description*.
5. Click *Save*.

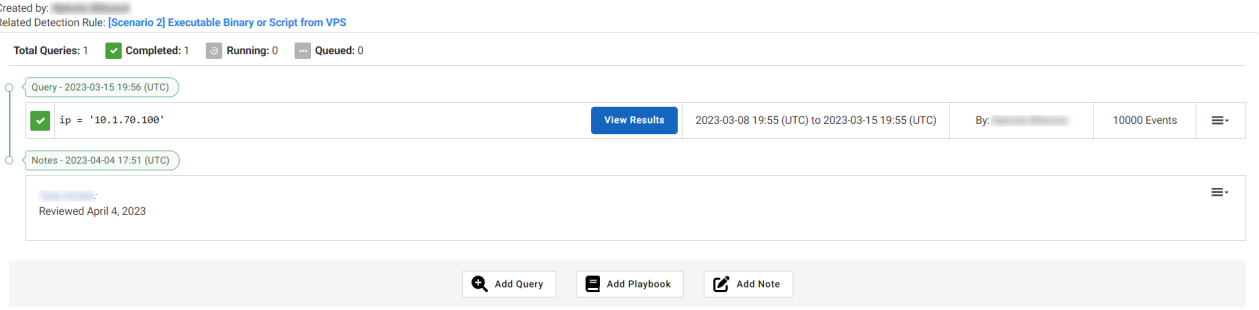
## Adding notes to an investigation

### To add a note to investigation:

1. Go to *Investigations > Investigate*.
2. Click *Select* to open an investigation.
3. Click *Add Note*. Optionally, you can click the *Add* menu (+) in the top-right of the page and select *Add Note*.



4. In the *Notes* field enter the details in plain text or markdown. Rendered markdown text will be visible. The note contents will be displayed along with the timestamp of when it was created.



**To update a note:**

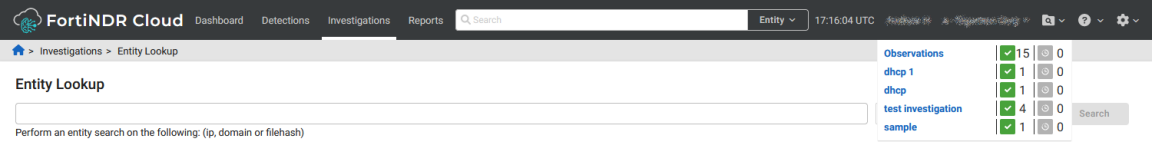
1. Click the Actions menu on the right side of the note and select *Update*.
2. Update the note and click *Update Note*.

**To delete a note:**

1. Click the Actions menu on the right side of the note and select *Delete*. The *Delete Note* dialog opens.
2. Click *Confirm*.

**Watch an investigation**

You can check the status of your query by clicking the *Notification* icon to the right of the account name in the top navigation. A panel displays the list of queries being watched, along with the number of queries completed and running. When the query is complete, you will see a green check mark in the top right corner.



**To watch an investigation:**

1. Go to *Investigations* and click *Select* to open the investigation you want to watch.
2. Click the *Not Watching* icon.

**To unwatch an investigation:**

1. Go to *Investigations* and click *Select* to open the investigation you want to watch.
2. Click the *Watching* icon.



## Facet Search

A *Facet* filters results of an IQL query in a pane adjacent to the main results table of an IQL query. A facet is an automatic filter that saves time configuring a search with the GUI.

The facet options are results-based attributes from a sample of the events found in the initial search. The facets will change based on the data in the records found by the search.

Faceted Searches are useful for getting a quick multidimensional view of the results to identify the most or least common elements.

You can enable Facets when:

- [Adding queries to an investigation on page 99](#)
- [Adding a playbook to an investigation on page 127](#)



Enabling facet search, may increase the time to process the query.

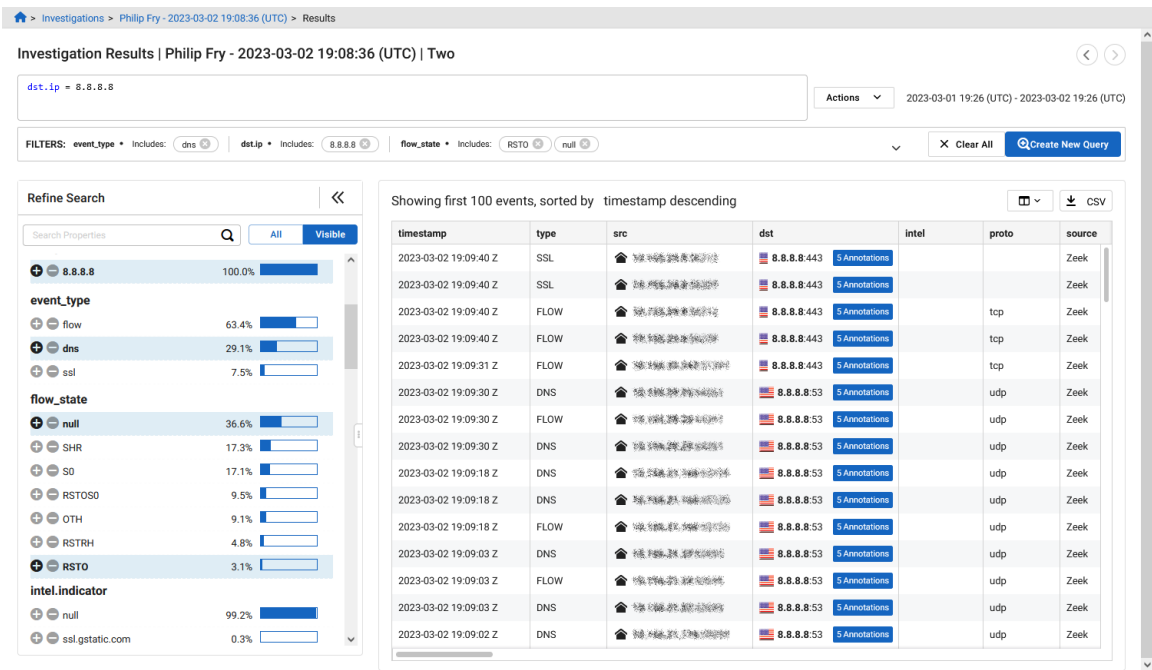
---

## Refine results using facet search

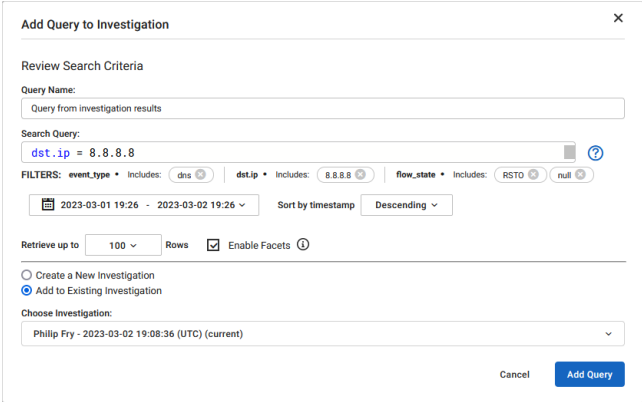
You can further refine your search on the results from the original query using facet search.

**To refine the results in a facet search:**

1. Click *Investigations*.
2. Click *Select* next to the investigation you want to open.
3. Click *View Results* for the facet search query you want to refine. The *Refine Search* pane displays a breakdown of the query results.



- Add or remove the filters based on your requirement. The selected filters appear under the original search query. You can also clear the selected filters by clicking *Clear All*.
- Click *Create New Query*.



- Create a new investigation or add the query to an existing investigation. By default, the new query is added to the current investigation.

|                                      |   |
|--------------------------------------|---|
| <b>Create a New Investigation</b>    | Select this option to create a new investigation. Enter the <i>Investigation Name</i> and <i>Description</i> . The default name for new investigations is the first and last name of the user creating the investigation as well as a date stamp of when the investigation was created. |
| <b>Add to Existing Investigation</b> | From the <i>Choose Investigation</i> dropdown, select an investigation.   |

- Click *Add Query*. The query and all the included and excluded facets will be shown in the investigation details page.



Philip Fry - 2023-03-02 19:08:36 (UTC)

Created by: Philip Fry

Total Queries: 5 ✔ Completed: 5 ⏸ Running: 0 ⏸ Queued: 0

- Query: test - 2023-03-02 19:23 (UTC)
  - ✔ `dst.ip = 8.8.8.8 group by dst.port` View Results 2023-03-01 19:22 (UTC) to 2023-03-02 19:22 (UTC) By: Philip Fry 100 Events
- Query: Two - 2023-03-02 19:26 (UTC)
  - ✔ `dst.ip = 8.8.8.8` View Results 2023-03-01 19:26 (UTC) to 2023-03-02 19:26 (UTC) By: Philip Fry 100 Events
- Query: boring - 2023-03-02 19:26 (UTC)
  - ✔ `src.ip = 8.8.8.8` View Results 2023-03-01 19:26 (UTC) to 2023-03-02 19:26 (UTC) By: Philip Fry 100 Events
- Query: day - 2023-03-02 19:28 (UTC)
  - ✔ `dst.ip = 8.8.8.8 group by DAY(timestamp)` View Results 2023-03-01 19:26 (UTC) to 2023-03-02 19:26 (UTC) By: Philip Fry 100 Events
- Query: Query from investigation results - 2023-03-02 19:38 (UTC)
  - ✔ `dst.ip = 8.8.8.8` No Results 2023-03-01 19:26 (UTC) to 2023-03-02 19:26 (UTC) By: Philip Fry 0 Events
  - FILTERS: event\_type Includes: dns dst.ip Includes: 8.8.8.8 flow\_state Includes: RSTO null

Add Query
Add Playbook
Add Note

## Tag and comment events

Use the *tag* column to communicate with members of the security team about an event in an investigation. Tags and comments are viewable to any user with access to the investigation. You can use s filter to view only tagged investigations or use the *Search* function to search for text in notes and comments.

Search

Search Timeline

dns:dst.ip = 8.8.8.8

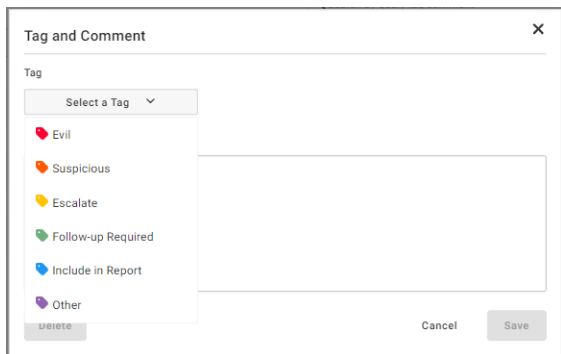
Last 24 Hours Sort by timestamp Descending Retrieve up to 100 Rows Enable Facets Search

Showing first 1 events, sorted by timestamp descending 
▼
□
↓ CSV

| tag   | timestamp             | type | src                                 | src.ip                                       | src.port                                 | src.internal                             | src.asn | src.asn.asn_org | src.asn.isp |
|---|-----------------------|------|-------------------------------------|--|--|--|---------|-----------------|-------------|
| <span style="color: green;">✔</span> <span style="color: grey;">🗨️</span> | 2023-05-25 17:29:59 Z | DNS  | <span style="color: grey;">🏠</span> | <span style="color: grey;">██████████</span> | <span style="color: grey;">██████</span> | <span style="color: grey;">██████</span> | True    |                 |             |

### To add a tag to an event:

- Do one of the following:
  - Click the *Investigations* tab, open an investigation and click *View Results*.
  - Go to *Investigations > Search timeline*. In the *Search Timeline* tab, click *View Results*.
- Click the *tag* column next to the event. The *Tag and Comment* dialog opens.



3. Select a tag from the dropdown.
4. (Optional) Add a comment to the event.
5. Click **Save**. The tag and comment icons are displayed in the *tag* column.

**To remove a tag from an event:**

1. Click the *tag* column next to the event. The *Tag and Comment* dialog opens.
2. Click *Delete* and then click *Confirm* in the dialog that opens.

## Viewing and filtering tagged events

Tagged events are displayed in the *Investigations* and *Search Timeline* tabs. Hover over a tag to see an overview of the tagged events in the investigation.

Investigations


Search by name and description

Tag: Escalate Tag: Evil Tag: Follow-up Required Tag: Include in Report Tag: Other Tag: Suspicious

| Name  | Description           | Created by              | Date Created           | Date Updated           | Activities   | Queries |
|---|-----------------------|-------------------------|------------------------|------------------------|--|---------|
| adhoc tag testing <span>Fortinet</span>         |                       | Max Nudol               | 2023-06-13 22:02 (UTC) | 2023-06-22 23:34 (UTC) | <span>20</span>  | 4       |
| Test For Tagging (Closed) <span>Fortinet</span> |                       | Max Nudol               | 2023-06-05 22:11 (UTC) | 2023-06-21 16:13 (UTC) | <span>Suspicious: 2<br/>Escalate: 6<br/>Follow-up Required: 2<br/>Include in Report: 4<br/>Other: 6</span> | 13      |
| Bobby Test - 2023-05-30 1...                    |                       | Bobby Test              | 2023-05-30 16:50 (UTC) | 2023-06-16 18:41 (UTC) |  | 2       |
| Test Rule Bobby Sun - 202...                    | <span>Fortinet</span> | Bobby Sun               | 2023-05-22 15:48 (UTC) | 2023-06-14 23:27 (UTC) | <span>1</span>   | 2       |
| Max Nudol - 2023-04-13 1...                     | <span>Fortinet</span> | Max Nudol               | 2023-04-13 16:50 (UTC) | 2023-06-19 22:48 (UTC) | <span>35</span>  | 34      |
| Creed Erickson - 2023-02-2...                   | <span>Fortinet</span> | Creed Erickson          | 2023-02-21 22:33 (UTC) | 2023-05-25 16:41 (UTC) | <span>13</span>  | 6       |
| jGy2b8sNFT9KxH4L0oEz6Z...                       | <span>Fortinet</span> | Ashok Raghunayakula     | 2022-09-24 00:38 (UTC) | 2023-06-19 22:12 (UTC) | <span>1</span>   | 92      |
| APT23 (Closed)                                  | At least not yet      | Jeremy (notify2) Hubble | 2022-06-15 19:26 (UTC) | 2023-06-21 17:11 (UTC) | <span>1</span>   | 91      |

**To use tags and notes to filter investigations:**

| Option                           | Description               |
|----------------------------------|---------------------------|
| <b>Go to Investigations &gt;</b> | 1. Click the Filter icon. |

| Option   | Description   |
|--|---|
| <b>Investigate</b>                               |  <ol style="list-style-type: none"> <li>In the <i>Tag</i> section, select <i>Tagged Investigations</i>.</li> <li>(Optional) To refine results, select a tab label from the list (such as <i>Evil</i>).</li> <li>Click the investigation name.</li> <li>(Optional) Click <i>Hide Notes</i> to only see the tags.</li> <li>Click <i>View Results</i>.</li> </ol>   |
| <b>Go to Investigations &gt; Search Timeline</b> | <ol style="list-style-type: none"> <li>Click the <i>All Queries</i> drop-down.</li> <li>In the <i>Tag</i> section, select <i>Tagged Investigations</i>.</li> <li>(Optional) To refine results, select a tab label from the list (such as <i>Evil</i>).</li> <li>Click <i>View Results</i>.</li> </ol>   |
| <b>Go to Investigations</b>                      | <ol style="list-style-type: none"> <li>Enter keywords in the <i>Search</i> field to search for text in comments and notes. Matching results are highlighted in yellow.</li> <li>Hover over the results in the <i>Activities</i> and <i>Notes</i> column. <ul style="list-style-type: none"> <li>Click a matched note to open the results table displaying the matched results.</li> <li>Click <i>View Details</i> to open the investigation. The matched text will be highlighted.</li> </ul> </li> </ol> |



After you filter the investigations, you can copy the URL to send the filtered view a member of your team.

## Packet Capture

*Packet Capture* tasks are defined and deployed on a per-sensor basis. A single task can be deployed to one, all, or any combination of sensors. Each sensor can spool up to four individual tasks, but only one task may run at once.

The active task will execute for 60 minutes or until it captures 1 MB of data, whichever comes first. Once either of those conditions are met, the active task will pause and the next spooled task will execute. The same task will begin again if it is the only one spooled. Tasks will continue to be spooled until they pass the specified expiration time or are terminated manually.

Packet capture tasks can have one of two states:

| State           | Description   |
|-----------------|---|
| <b>Active</b>   | The task is currently in rotation for execution.                              |
| <b>Inactive</b> | The task has reached the requested end time or has been terminated by a user. |

Packet capture tasks can be created, viewed, or terminated from the *Packet Capture* page. All tasks, both *Active* and *Inactive*, are displayed by default.

Investigations > Packet Capture

Packet Capture

Showing 1 - 2 out of 2 tasks.

Search   Has Files  Hide Inactive

|  |   |
|--|---|
| <p>http web traffic</p> <p>STATUS: <span style="background-color: #0070C0; color: white; padding: 2px;">ACTIVE</span> FILES CAPTURED: <span style="background-color: #808080; color: white; padding: 2px;">0</span> SENSORS: All CREATED: 2023-02-22 17:26 (UTC)</p> | ☰ |
| <p>rCMD test</p> <p>STATUS: <span style="background-color: #808080; color: white; padding: 2px;">INACTIVE</span> FILES CAPTURED: <span style="background-color: #808080; color: white; padding: 2px;">0</span> SENSORS: All CREATED: 2020-05-27 18:31 (UTC)</p>      | ☰ |

## Reviewing a task

Click a task on the page to view metadata for the task and any PCAP data captured. Each execution of a task will produce exactly one log file and one PCAP.

- The log file will specify the start and end times of the respective execution .
- The PCAP will contain any captured traffic.

The PCAP will be empty if no traffic matched the BPF. Each file collected as part of the PCAP task can then be downloaded and viewed within WireShark or another preferred PCAP analysis tool. You can adjust which files are displayed (only PCAP, all PCAP, only non-empty PCAP) by checking or unchecking the respective options on the task page.

Investigations > Packet Capture > 29-ssl

Packet Capture

29-ssl

STATUS: ACTIVE FILES CAPTURED: 6 SENSORS: git29

BPF: port 443

START TIME: 2023-02-14 16:12 (UTC) END TIME: 2023-02-14 17:12 (UTC) CREATED BY: [Anshu Kishore@paloaltonetworks.com](#) CREATED: 2023-02-14 16:12 (UTC)

Files  Show Empty Files  Show PCAP Only

| Name                          | ▲ Size      | Created                | Download                 |
|-------------------------------|-------------|------------------------|--------------------------|
| git29-1676391187-activity.log | 190 Bytes   | 2023-02-14 16:13 (UTC) | <a href="#">Download</a> |
| git29-1676391187-pcap.enc     | 1012.67 KB  | 2023-02-14 16:13 (UTC) | <a href="#">Download</a> |
| git29-1676392100-activity.log | 12.209 KB   | 2023-02-14 16:28 (UTC) | <a href="#">Download</a> |
| git29-1676392100-pcap.enc     | 998.997 KB  | 2023-02-14 16:28 (UTC) | <a href="#">Download</a> |
| git29-1676392539-activity.log | 23.358 KB   | 2023-02-14 16:35 (UTC) | <a href="#">Download</a> |
| git29-1676392539-pcap.enc     | 1017.426 KB | 2023-02-14 16:35 (UTC) | <a href="#">Download</a> |

## Creating a Packet Capture

To create a new task, the selected account should have one or more sensors with the PCAP feature enabled.

### To create a Packet Capture task:

1. Go to *Investigations > Packet Capture*.
2. Click Create Task. The *Create New Packet Capture Task* window opens.

3. Configure the task settings.

| Field       | Required | Description   |
|-------------|----------|---|
| Title       | Yes      | The name of the task.   |
| BPF         | Yes      | The BPF for traffic to match.   |
| Date Range  | Yes      | The interval that the task will be active for, default = the next 24 hours. |
| Sensors     | No       | The sensors that the task will run on, default = All Sensors.               |
| Description | No       | A description of the task.  |

**Create new Packet Capture Task** ✕

**i**

- A maximum of 4 tasks can be active on a given sensor at once.
- A maximum of 1MB of PCAP data will be gathered per task.

Title \*

BPF \*

Date Range \*

Sensors

All Sensors

Description

A description of what this task does.



Sensors can only spool four (4) tasks at once, so only specify sensors that the task is relevant to. For example, if you are trying to troubleshoot one particular host in a particular data center, you probably only need to deploy the task to one sensor.

4. Click *Create*.

## Terminating and deleting Packet Captures

### To terminate a Packet Capture task:

1. Go to *Investigations > Packet Capture*.
2. Click the *Actions* menu at the right side of the task and click *Terminate Task*. A confirmation dialog opens.

[Home](#) > [Investigations](#) > [Packet Capture](#)

**Packet Capture**

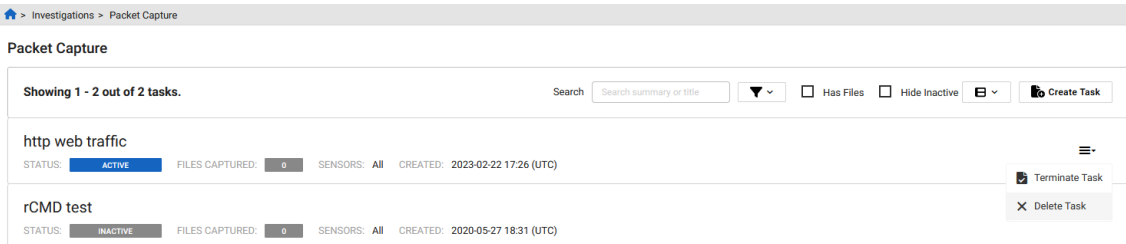
Showing 1 - 2 out of 2 tasks. Search  ▼  Has Files  Hide Inactive

|  |   |
|--|---|
| <p><b>http web traffic</b></p> <p>STATUS: <span style="background-color: #0070c0; color: white; padding: 2px;">ACTIVE</span> FILES CAPTURED: <span style="background-color: #ccc; padding: 2px;">0</span> SENSORS: All CREATED: 2023-02-22 17:26 (UTC)</p> | <span style="font-size: 1.2em;">☰</span><br><input type="button" value="Terminate Task"/> |
| <p><b>rCMD test</b></p> <p>STATUS: <span style="background-color: #ccc; padding: 2px;">INACTIVE</span> FILES CAPTURED: <span style="background-color: #ccc; padding: 2px;">0</span> SENSORS: All CREATED: 2020-05-27 18:31 (UTC)</p>                       | <input type="button" value="Delete Task"/>  |

3. Click *Confirm*. The task changes to *Inactive*.

**To delete a Packet Capture:**

1. Go to *Investigate > Packet Capture*.
2. Click the *Actions* menu at the right side of the task and click *Delete*. A confirmation dialog opens.



3. Click *Confirm*.

**BPF resources**

For in-depth information on Berkeley Packet Filters (BPFs), see The Linux Kernel Archives web site at <https://www.kernel.org/>. You can also download the BPF reference guide from [here](#).

| SYNTAX   |                                   |  |                           |  |                                    |
|--|-----------------------------------|--|---------------------------|--|------------------------------------|
| [Protocol] [Direction] [Type] {ip/subnet/port/portrange}   |                                   |  |                           |  |                                    |
| PROTOCOL   |                                   | DIRECTION  |                           | TYPE   |                                    |
| <i>Limit the match to a specific protocol. If no protocol is supplied, all protocols consistent with the type are assumed.</i> |                                   | <i>Transfer direction to and/or from the type. If no direction is supplied, 'src or dst' is assumed.</i> |                           | <i>Type of entity, port, or range of ports. If no type is supplied, host is assumed.</i> |                                    |
| ether  | ethernet                          | src or dst (default)   | source or destination     | host (default)   | ip address                         |
| fddi   | alias for ether                   | src and dst  | source and destination    | net  | ip address or subnet               |
| icmp   | internet control message protocol | src  | source only               | port   | tcp/udp port number                |
| wlan   | wireless lan; alias for ether     | dst  | destination only          | portrange  | range of tcp/udp ports (xxxx-xxxx) |
| ip   | ipv4                              | [proto] broadcast  | proto must be ip or ether |  |                                    |
| ip6  | ipv6                              | OPERATORS  |                           |  |                                    |
| arp  | address resolution protocol       | '='  | equal to                  | '  ' 'or'  | logical or                         |
| tcp  | transmission control protocol     | '!' or 'not'   | not equal to              | '<' 'less'   | less than                          |
| udp  | user datagram protocol            | '&&' 'and'   | logical and               | '>' 'greater'  | greater than                       |

| COMMON EXPRESSIONS   |  |
|--|--|
| host xxx.xxx.xxx.xxx   | all packets to/from a host   |
| src host xxx.xxx.xxx.xxx && dst host xxx.xxx.xxx.xxx                         | all packets from a source host to a destination host                                 |
| dst port 23  | all packets to port 23 (telnet)  |
| udp src net xxx.xxx.xxx && dst host xxx.xxx.xxx.xxx                          | only udp packets from a dotted pair subnet to destination host                       |
| ip6 && not net xxx.xxx.xxx   | only IPv6 packets outside of a dotted triple subnet                                  |
| src host xxx.xxx.xxx.xxx && (dst portrange xxxx-xxxx && dst net xxx.xxx.xxx) | all packets from a source host to a destination port range in a dotted triple subnet |
| dst portrange 49152-65535 && gateway xxx.xxx.xxx.xxx                         | all packets to non-standard ports on a gateway                                       |
| host xxx.xxx.xxx.xxx    host xxx.xxx.xxx.xxx                                 | all packets to/from host A or host B   |

| BYTE LEVEL FILTERING    |   |
|-------------------------|---|
| ip[9]!=47               | <i>all packets where IP protocol field is GRE (tunnel)</i>            |
| ip[8]<64                | <i>all packets where IP time-to-live (TTL) is less than 64</i>        |
| icmp[0]=3               | <i>all packets with ICMP message type 3 (destination unreachable)</i> |
| tcp[13]=32    tcp[13]=8 | <i>all packets with TCP flags set to PSH or URG</i>                   |

| HOW TO READ PACKET HEADERS |   |   |   |          |   |   |   |               |   |   |    |          |    |    |    |               |    |    |    |          |    |    |    |               |    |    |    |          |    |    |    |    |
|----------------------------|---|---|---|----------|---|---|---|---------------|---|---|----|----------|----|----|----|---------------|----|----|----|----------|----|----|----|---------------|----|----|----|----------|----|----|----|----|
| Word 0                     |   |   |   |          |   |   |   |               |   |   |    |          |    |    |    |               |    |    |    |          |    |    |    |               |    |    |    |          |    |    |    |    |
| Byte Offset 0              |   |   |   |          |   |   |   | Byte Offset 1 |   |   |    |          |    |    |    | Byte Offset 2 |    |    |    |          |    |    |    | Byte Offset 3 |    |    |    |          |    |    |    |    |
| Nibble 0                   |   |   |   | Nibble 1 |   |   |   | Nibble 2      |   |   |    | Nibble 3 |    |    |    | Nibble 4      |    |    |    | Nibble 5 |    |    |    | Nibble 6      |    |    |    | Nibble 7 |    |    |    |    |
| BIT                        | 0 | 1 | 2 | 3        | 4 | 5 | 6 | 7             | 8 | 9 | 10 | 11       | 12 | 13 | 14 | 15            | 16 | 17 | 18 | 19       | 20 | 21 | 22 | 23            | 24 | 25 | 26 | 27       | 28 | 29 | 30 | 31 |

| TCP HEADER - RFC 793   |   |   |   |          |   |   |   |           |     |     |     |     |     |     |     |                         |    |    |    |    |    |    |    |           |    |    |    |    |    |    |    |
|------------------------|---|---|---|----------|---|---|---|-----------|-----|-----|-----|-----|-----|-----|-----|-------------------------|----|----|----|----|----|----|----|-----------|----|----|----|----|----|----|----|
| 0                      | 1 | 2 | 3 | 4        | 5 | 6 | 7 | 8         | 9   | 10  | 11  | 12  | 13  | 14  | 15  | 16                      | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24        | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| Offset 0               |   |   |   |          |   |   |   | Offset 1  |     |     |     |     |     |     |     | Offset 2                |    |    |    |    |    |    |    | Offset 3  |    |    |    |    |    |    |    |
| Source Port Number     |   |   |   |          |   |   |   |           |     |     |     |     |     |     |     | Destination Port Number |    |    |    |    |    |    |    |           |    |    |    |    |    |    |    |
| Offset 4               |   |   |   |          |   |   |   | Offset 5  |     |     |     |     |     |     |     | Offset 6                |    |    |    |    |    |    |    | Offset 7  |    |    |    |    |    |    |    |
| Sequence Number        |   |   |   |          |   |   |   |           |     |     |     |     |     |     |     |                         |    |    |    |    |    |    |    |           |    |    |    |    |    |    |    |
| Offset 8               |   |   |   |          |   |   |   | Offset 9  |     |     |     |     |     |     |     | Offset 10               |    |    |    |    |    |    |    | Offset 11 |    |    |    |    |    |    |    |
| Acknowledgement Number |   |   |   |          |   |   |   |           |     |     |     |     |     |     |     |                         |    |    |    |    |    |    |    |           |    |    |    |    |    |    |    |
| Offset 12              |   |   |   |          |   |   |   | Offset 13 |     |     |     |     |     |     |     | Offset 14               |    |    |    |    |    |    |    | Offset 15 |    |    |    |    |    |    |    |
| Header Length          |   |   |   | Reserved |   |   |   | CWR       | ECE | URG | ACK | PSH | RST | SYN | FIN | Window Size             |    |    |    |    |    |    |    |           |    |    |    |    |    |    |    |
| Offset 16              |   |   |   |          |   |   |   | Offset 17 |     |     |     |     |     |     |     | Offset 18               |    |    |    |    |    |    |    | Offset 19 |    |    |    |    |    |    |    |
| Checksum               |   |   |   |          |   |   |   |           |     |     |     |     |     |     |     | Urgent Pointer          |    |    |    |    |    |    |    |           |    |    |    |    |    |    |    |
| Offset 20              |   |   |   |          |   |   |   | Offset 21 |     |     |     |     |     |     |     | Offset 22               |    |    |    |    |    |    |    | Offset 23 |    |    |    |    |    |    |    |
| TCP Options            |   |   |   |          |   |   |   |           |     |     |     |     |     |     |     |                         |    |    |    |    |    |    |    |           |    |    |    |    |    |    |    |
| Data                   |   |   |   |          |   |   |   |           |     |     |     |     |     |     |     |                         |    |    |    |    |    |    |    |           |    |    |    |    |    |    |    |

| UDP HEADER - RFC 768 |   |   |   |   |   |   |   |          |   |    |    |    |    |    |    |                         |    |    |    |    |    |    |    |           |    |    |    |    |    |    |    |
|----------------------|---|---|---|---|---|---|---|----------|---|----|----|----|----|----|----|-------------------------|----|----|----|----|----|----|----|-----------|----|----|----|----|----|----|----|
| 0                    | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8        | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16                      | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24        | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| Offset 0             |   |   |   |   |   |   |   | Offset 1 |   |    |    |    |    |    |    | Offset 2                |    |    |    |    |    |    |    | Offset 3  |    |    |    |    |    |    |    |
| Source Port Number   |   |   |   |   |   |   |   |          |   |    |    |    |    |    |    | Destination Port Number |    |    |    |    |    |    |    |           |    |    |    |    |    |    |    |
| Offset 4             |   |   |   |   |   |   |   | Offset 5 |   |    |    |    |    |    |    | Offset 6                |    |    |    |    |    |    |    | Offset 7  |    |    |    |    |    |    |    |
| Length               |   |   |   |   |   |   |   |          |   |    |    |    |    |    |    | Checksum                |    |    |    |    |    |    |    |           |    |    |    |    |    |    |    |
| Offset 8             |   |   |   |   |   |   |   | Offset 9 |   |    |    |    |    |    |    | Offset 10               |    |    |    |    |    |    |    | Offset 11 |    |    |    |    |    |    |    |
| Data                 |   |   |   |   |   |   |   |          |   |    |    |    |    |    |    |                         |    |    |    |    |    |    |    |           |    |    |    |    |    |    |    |

| ICMP HEADER - RFC 792                          |   |   |   |   |   |   |   |              |   |    |    |    |    |    |    |          |    |    |    |    |    |    |    |          |    |    |    |    |    |    |    |
|--|---|---|---|---|---|---|---|--------------|---|----|----|----|----|----|----|----------|----|----|----|----|----|----|----|----------|----|----|----|----|----|----|----|
| 0  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8            | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16       | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24       | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| Offset 0                                       |   |   |   |   |   |   |   | Offset 1     |   |    |    |    |    |    |    | Offset 2 |    |    |    |    |    |    |    | Offset 3 |    |    |    |    |    |    |    |
| Message Type                                   |   |   |   |   |   |   |   | Message Code |   |    |    |    |    |    |    | Checksum |    |    |    |    |    |    |    |          |    |    |    |    |    |    |    |
| Offset 4                                       |   |   |   |   |   |   |   | Offset 5     |   |    |    |    |    |    |    | Offset 6 |    |    |    |    |    |    |    | Offset 7 |    |    |    |    |    |    |    |
| (Variable Contents Depending on Type and Code) |   |   |   |   |   |   |   |              |   |    |    |    |    |    |    |          |    |    |    |    |    |    |    |          |    |    |    |    |    |    |    |

| IPv4 HEADER – RFC 791    |   |                  |   |                 |   |   |   |                           |   |    |    |           |    |    |    |    |    |    |                 |    |    |    |    |    |    |    |    |    |    |    |    |  |  |
|--------------------------|---|------------------|---|-----------------|---|---|---|---------------------------|---|----|----|-----------|----|----|----|----|----|----|-----------------|----|----|----|----|----|----|----|----|----|----|----|----|--|--|
| 0                        | 1 | 2                | 3 | 4               | 5 | 6 | 7 | 8                         | 9 | 10 | 11 | 12        | 13 | 14 | 15 | 16 | 17 | 18 | 19              | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |  |  |
| Offset 0                 |   |                  |   | Offset 1        |   |   |   | Offset 2                  |   |    |    | Offset 3  |    |    |    |    |    |    |                 |    |    |    |    |    |    |    |    |    |    |    |    |  |  |
| Version                  |   | IP Header Length |   | Type of Service |   |   |   | Total Length (in Offsets) |   |    |    |           |    |    |    |    |    |    |                 |    |    |    |    |    |    |    |    |    |    |    |    |  |  |
| Offset 4                 |   |                  |   | Offset 5        |   |   |   | Offset 6                  |   |    |    | Offset 7  |    |    |    |    |    |    |                 |    |    |    |    |    |    |    |    |    |    |    |    |  |  |
| IP Identification Number |   |                  |   |                 |   |   |   |                           |   |    |    |           |    |    |    | x  | D  | M  | Fragment Offset |    |    |    |    |    |    |    |    |    |    |    |    |  |  |
| Offset 8                 |   |                  |   | Offset 9        |   |   |   | Offset 10                 |   |    |    | Offset 11 |    |    |    |    |    |    |                 |    |    |    |    |    |    |    |    |    |    |    |    |  |  |
| Time to Live (TTL)       |   |                  |   | Protocol        |   |   |   | Header Checksum           |   |    |    |           |    |    |    |    |    |    |                 |    |    |    |    |    |    |    |    |    |    |    |    |  |  |
| Offset 12                |   |                  |   | Offset 13       |   |   |   | Offset 14                 |   |    |    | Offset 15 |    |    |    |    |    |    |                 |    |    |    |    |    |    |    |    |    |    |    |    |  |  |
| Source IP Address        |   |                  |   |                 |   |   |   |                           |   |    |    |           |    |    |    |    |    |    |                 |    |    |    |    |    |    |    |    |    |    |    |    |  |  |
| Offset 16                |   |                  |   | Offset 17       |   |   |   | Offset 18                 |   |    |    | Offset 19 |    |    |    |    |    |    |                 |    |    |    |    |    |    |    |    |    |    |    |    |  |  |
| Destination IP Address   |   |                  |   |                 |   |   |   |                           |   |    |    |           |    |    |    |    |    |    |                 |    |    |    |    |    |    |    |    |    |    |    |    |  |  |
| Offset 20                |   |                  |   | Offset 21       |   |   |   | Offset 22                 |   |    |    | Offset 23 |    |    |    |    |    |    |                 |    |    |    |    |    |    |    |    |    |    |    |    |  |  |
| IP Options               |   |                  |   |                 |   |   |   |                           |   |    |    |           |    |    |    |    |    |    |                 |    |    |    |    |    |    |    |    |    |    |    |    |  |  |
| Data                     |   |                  |   |                 |   |   |   |                           |   |    |    |           |    |    |    |    |    |    |                 |    |    |    |    |    |    |    |    |    |    |    |    |  |  |

FLAGS  
 x = Reserved    D = Do Not Fragment    M = More Fragments Follow

| IPv6 HEADER – RFC 2460             |   |               |   |                              |   |            |   |             |   |    |    |           |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|------------------------------------|---|---------------|---|------------------------------|---|------------|---|-------------|---|----|----|-----------|----|----|----|-----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0                                  | 1 | 2             | 3 | 4                            | 5 | 6          | 7 | 8           | 9 | 10 | 11 | 12        | 13 | 14 | 15 | 16        | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| Offset 0                           |   |               |   | Offset 1                     |   |            |   | Offset 2    |   |    |    | Offset 3  |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Version                            |   | Traffic Class |   |                              |   | Flow Label |   |             |   |    |    |           |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Offset 4                           |   |               |   | Offset 5                     |   |            |   | Offset 6    |   |    |    | Offset 7  |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Payload Length                     |   |               |   |                              |   |            |   | Next Header |   |    |    |           |    |    |    | Hop Limit |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Offset 8                           |   |               |   | Offset 9                     |   |            |   | Offset 10   |   |    |    | Offset 11 |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Source IP Address                  |   |               |   |                              |   |            |   |             |   |    |    |           |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Offset 12                          |   |               |   | Offset 13                    |   |            |   | Offset 14   |   |    |    | Offset 15 |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Source IP Address (continued)      |   |               |   |                              |   |            |   |             |   |    |    |           |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Offset 16                          |   |               |   | Offset 17                    |   |            |   | Offset 18   |   |    |    | Offset 19 |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Source IP Address (continued)      |   |               |   |                              |   |            |   |             |   |    |    |           |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Offset 20                          |   |               |   | Offset 21                    |   |            |   | Offset 22   |   |    |    | Offset 23 |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Source IP Address (continued)      |   |               |   |                              |   |            |   |             |   |    |    |           |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Offset 24                          |   |               |   | Offset 25                    |   |            |   | Offset 26   |   |    |    | Offset 27 |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Destination IP Address             |   |               |   |                              |   |            |   |             |   |    |    |           |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Offset 28                          |   |               |   | Offset 29                    |   |            |   | Offset 30   |   |    |    | Offset 31 |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Destination IP Address (continued) |   |               |   |                              |   |            |   |             |   |    |    |           |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Offset 32                          |   |               |   | Offset 33                    |   |            |   | Offset 34   |   |    |    | Offset 35 |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Destination IP Address (continued) |   |               |   |                              |   |            |   |             |   |    |    |           |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Offset 36                          |   |               |   | Offset 37                    |   |            |   | Offset 38   |   |    |    | Offset 39 |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Destination IP Address (continued) |   |               |   |                              |   |            |   |             |   |    |    |           |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Offset 40                          |   |               |   | Offset 41                    |   |            |   | Offset 42   |   |    |    | Offset 43 |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Net Header                         |   |               |   | Extension Header Information |   |            |   |             |   |    |    |           |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Extension Header                   |   |               |   |                              |   |            |   |             |   |    |    |           |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Data                               |   |               |   |                              |   |            |   |             |   |    |    |           |    |    |    |           |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |

## PCAP encryption

FortiNDR Cloud requires the encryption of all PCAP data captured and stored on the platform, backed by public key cryptography. Adding a PEM-encoded RSA key to an account on the Account management page will enable this feature.





Activation of the PCAP encryption feature prevents FortiNDR Cloud analysts from reviewing the contents of any captured packet data, and renders that data unrecoverable should the private key associated with the uploaded public key be lost.

---

## Generating a key



Be sure to only upload the contents of the `public.pem` file and keep the `private.pem` file safe. In the event that `private.pem` is lost, FortiNDR Cloud is unable to recover either it or the contents of any PCAP encrypted with the matching public key

---

For instructions on how to upload the generated public key, see the [Settings on page 135](#) page.

## Windows

To generate a key pair on Windows, we recommended using the PCAPUtil program. You can download the binary [here](#) or from [Settings \(Account Management\) on page 151](#) in [Account management on page 146](#).

---



You must be logged in to FortiNDR Cloud to download the binary.

---

Generate a key pair with files named `public.pem` (public key) and `private.pem` (private key) in the current directory. PCAPUtil supports overriding all file names and locations via command line arguments.

```
bash
pcaputil generate
```

## macOS and Linux

Generate a public/private key pair using the built-in OpenSSL library.

```
bash
openssl genrsa -out private.pem 4096
openssl rsa -in private.pem -outform PEM -pubout -out public.pem
```

## Decrypting a PCAP

Unencrypted PCAP files are denoted with an extension of `.pcap`, and encrypted PCAP files are denoted with the extension `.pcap.enc`.

## Windows

Encrypted PCAP files can be decrypted with the FortiNDR Cloud [PCAPUtil](#) binary.



You must be logged in to FortiNDR Cloud to access this file.

```
pcaputil decrypt -private private.pem -src sen1-1502499443.pcap.enc -dst sen1-1502499443.pcap
```

## macOS and Linux

Use the following script to extract and decrypt the PCAP:

```
bash
#!/usr/bin/env bash
show_help () {
echo "Usage: $0 private_key encrypted_pcap decrypted_pcap"
}
if [ -z $3 ]; then
show_help
exit 0
fi
tar xzf $2
openssl rsautl -decrypt -inkey $1 -in session.key.enc -out session.key
key=$(xxd -p -c 96 session.key | cut -c 1-64)
iv=$(xxd -p -c 96 session.key | cut -c 65-96)
openssl enc -aes-256-cbc -d -in data -out $3 -nosalt -K $key -iv $iv
rm data
rm session.key
rm session.key.enc
```

## Managing encryption keys

Any PCAP captured and stored in FortiNDR Cloud will be encrypted by adding the associated keys to the account.

FortiNDR Cloud requires the encryption of all PCAP data captured and stored on the platform, backed by public key cryptography.

### Encryption key requirement impact on existing sensors

|   |   |
|---|---|
| <b>If you do not have a PCAP-enabled sensor</b> | The encryption key will be required to enable PCAP on sensors   |
| <b>If you have a PCAP-enabled sensor</b>        | <ul style="list-style-type: none"> <li>• There is no change in behavior for existing PCAP-enabled sensors.</li> <li>• After the encryption key is provided, the PCAP-enabled sensor will upload encrypted PCAP files.</li> <li>• For existing PCAP-enabled sensors that are capturing without a key, you should still be able to disable them without a key.</li> <li>• Encryption keys can be updated directly without needing to delete an existing key. Existing behaviors and PCAP-enabled sensors will not be impacted.</li> </ul> |
| <b>When deleting the encryption</b>             | <ul style="list-style-type: none"> <li>• PCAP will be disabled on all the sensors for this account.</li> </ul>  |

- key**
- All PCAP upload requests for those sensors will be silently ignored.
  - When the encryption key is provided again after it's been deleted, you will need to enable PCAP on the sensor manually.

## Enabling PCAP on a sensor requires encryption

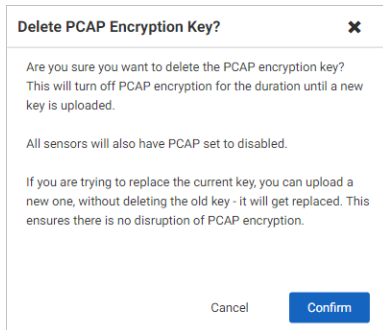
When enabling PCAP on an individual sensor, the *PCAP Enabled* option is disabled unless you have encryption enabled and display a note advising that you must enable encryption before enabling PCAP.

Warning appears on Sensor Update dialog accessed from the list of sensors:

Warning appears on the detailed Sensor Settings page:

## Deleting a PCAP encryption key

When deleting a PCAP key for an account, a warning will appear advising that PCAP will be disabled for sensors associated with that account.

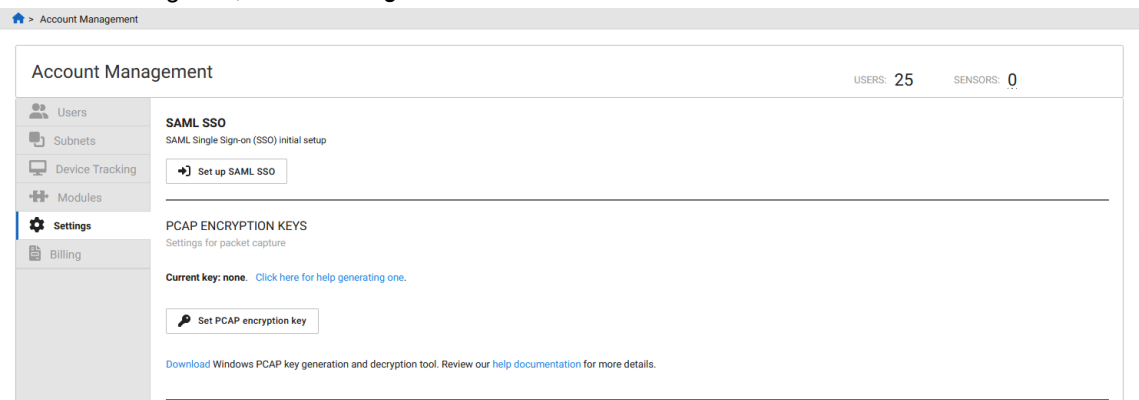


Click *Confirm* to acknowledge the message and proceed.

## Encryption key settings

**To access PCAP Encryption Keys settings:**

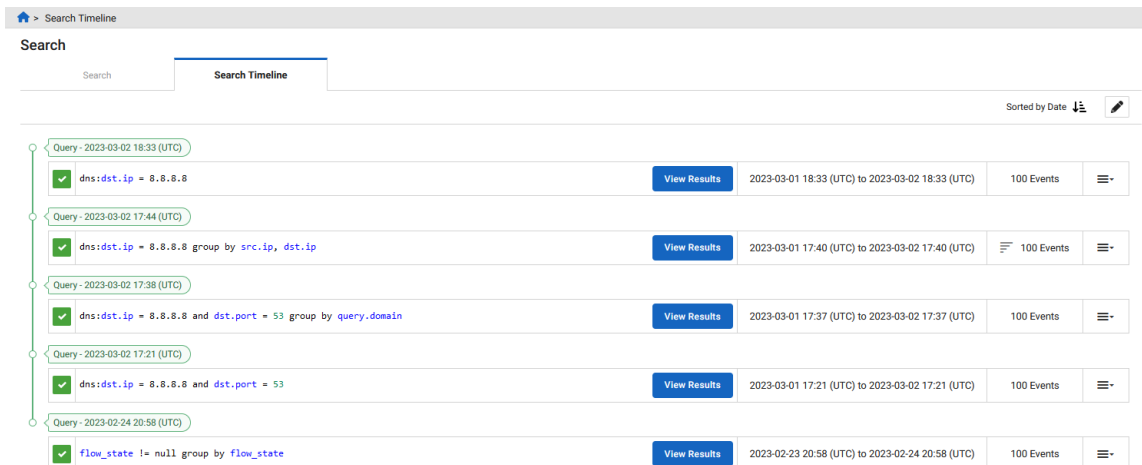
1. Click on the gear icon on the top right and select *Account Management*.
2. Select an account.
3. On the left navigation, select *Settings*.



The *Set PCAP encryption key* button will only appear for the Admin role.

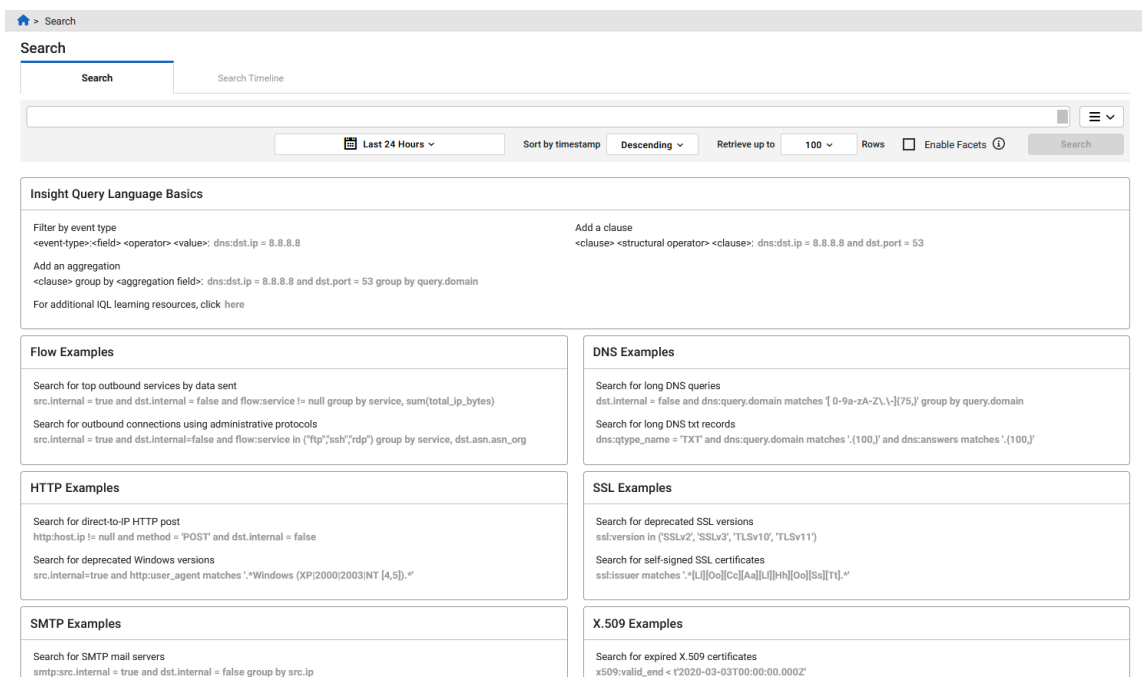
## Search Timeline

The *Search Timeline* page shows the history of Adhoc queries. Use this page to view the query status, past query results, delete query, and create detection out of the selected Adhoc query.



The Search tab

contains example queries of topics such as Flow, DNS, X.509, RDP, HTTP, SSH, SMTP, FTP, SSL, Kerberos, SMB, NTLM, DCE-RPC and PE are added. You can click any of the example queries, modify them, and then perform the search operation.



## Creating queries with Search Timeline

Privately search and iterate over recent events. You can quickly modify and re-run the queries. You can use a query in Search Timeline to create a new detection rule or investigation, or use the query in an existing investigation.

### To perform a search:

1. Go to *Investigations > Search Timeline*.
2. Click the *Search* tab.

- Enter the query in the search box using one of the following options:
  - Enter the IQL query in the *Search* field. By default, you can view the results of the events that occurred in the last 24 hours.
  - Click an example search string to add it to the Search field.

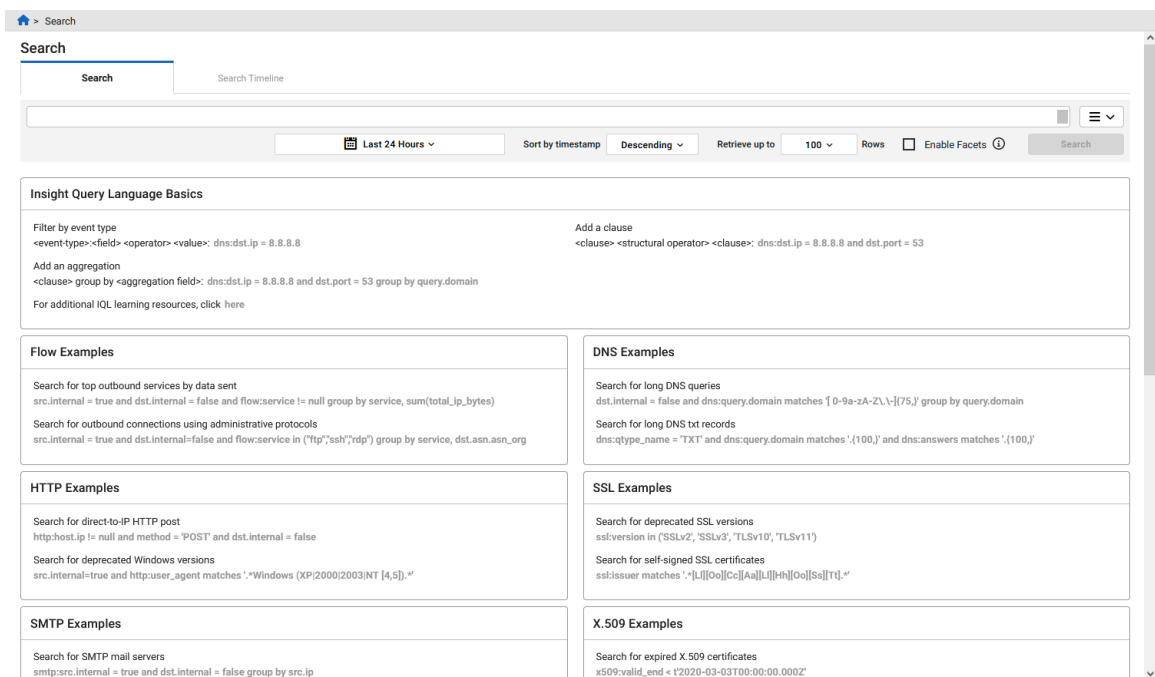
**Flow Examples**

Search for top outbound services by data sent  
`src.internal = true and dst.internal = false and flow:service != null group by service, sum(total_ip_bytes)`

Search for outbound connections using administrative protocols  
`src.internal = true and dst.internal=false and flow:service in ("ftp","ssh","rdp") group by service, dst.asn.asn_org`

- Configure the search settings.

|                                      |   |
|--------------------------------------|---|
| <b>Date range</b>                    | Use the date picker to configure the date range or select <i>Last Hour</i> , <i>Last 24 Hours</i> , or <i>Last 7 days</i> and click <i>Apply</i> .<br>You can select any time period within the last 365 days as long as it is limited to seven days. |
| <b>Sort by timestamp</b>             | Select <i>Ascending</i> or <i>Descending</i> .  |
| <b>Retrieve up to xxx Rows</b>       | Select <i>100</i> , <i>500</i> or <i>1,000</i> rows.  |
| <b>Add to Existing Investigation</b> | From the <i>Choose Investigation</i> dropdown, select an investigation.   |
| <b>Enable Facets</b>                 | Select to return the panel that allows narrowing the search. This may make the query longer to complete. For more information, see <a href="#">Facet Search on page 103</a> .   |



- Click *Search*.

**To move Search Timeline queries to Investigations:**


1. Click Investigations > Search Timeline.
2. Click the *Search Timeline* tab.

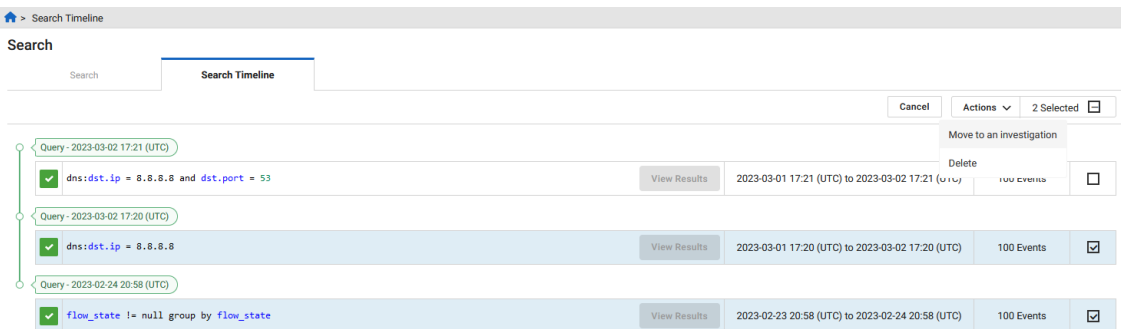
**To move a query**

Click the Actions menu at the end of the row and select *Move to an Investigation*.



**To move multiple queries**

1. Click the Edit button and select the queries to be moved.
- 
2. Click *Actions > Move to an Investigation*.



3. Create a new investigation or add the query to an existing investigation.

**Create a New Investigation**

Select this option to create a new investigation. Enter the *Investigation Name* and *Description*. The default name for new investigations is the first and last name of the user creating the investigation as well as a date stamp of when the investigation was created.

**Add to Existing Investigation**

From the *Choose Investigation* dropdown, select an investigation.

4. Click *Move*.

**To delete queries in the Search Timeline tab:**


1. Click Investigations > Search Timeline.
2. Click the *Search Timeline* tab.

**To delete a query**

Click the Actions menu at the end of the row and select *Delete Query*.



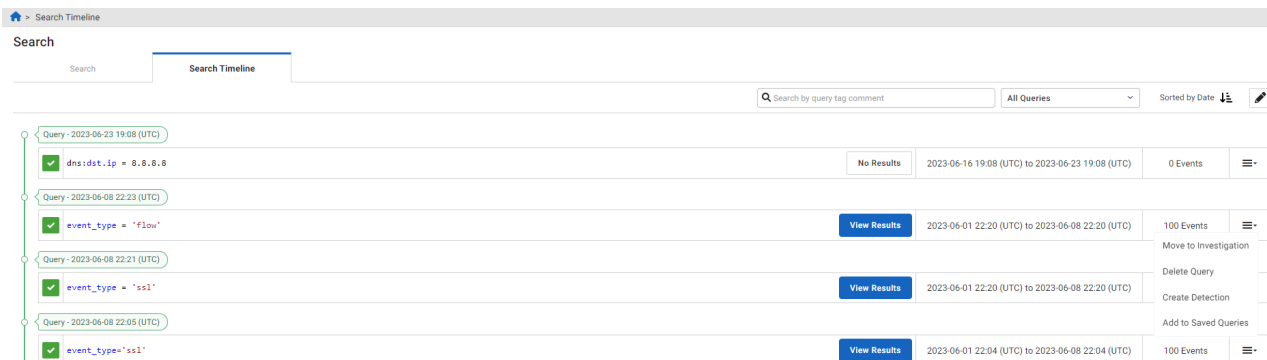
**To delete multiple queries**

1. Click the Edit button and select the queries to be deleted.
- 
2. Click *Actions > Delete Query*.

3. In the confirmation dialog, click *Confirm*.

**To create detection from an adhoc query:**

1. Click the *Search Timeline* tab.
2. Click the Actions menu at the end of the row and click *Create Detection*. The *Create A Detection Rule* page opens.



3. Configure the detection rule. See, [Creating a rule on page 71](#).

**To save a query:**

1. Click the *Search Timeline* tab.
2. Click the Actions menu at the end of the row and click *Add to Saved Queries*. The *Save Query* dialog opens.
3. Enter the query details and click *Save*.

|                     |                                   |
|---------------------|-----------------------------------|
| <b>Query Name</b>   | Enter a name for the query.       |
| <b>Search Query</b> | This field cannot be edited.      |
| <b>Description</b>  | Enter a description of the query. |



You can use a saved query when you create a new rule or investigation.

## IQL Operators

The following operators are supported in IQL.

- [Comparison operators on page 121](#)
- [Logical operators on page 121](#)
- [Exclude operators on page 122](#)
- [Pattern operators on page 122](#)
- [Units on page 122](#)
- [Supported units on page 123](#)
- [Fields with units on page 123](#)



## Comparison operators

Comparison operators are used to compare fields to values. The following comparison operators are supported by IQL.

| Operator | Description  | Example                               |
|----------|--|---------------------------------------|
| =, ==    | Equals   | <code>ip = 8.8.8.8</code>             |
| !=, <>   | Does not equal   | <code>ip != 8.8.8.8</code>            |
| IN       | Set/list operator - the field matches any of the listed values | <code>ip IN (8.8.8.8, 8.8.4.4)</code> |
| >        | Greater than   | <code>ip_bytes &gt; 100</code>        |
| <        | Less than  | <code>ip_bytes &lt; 100</code>        |
| >=       | Greater than or equal to                                       | <code>ip_bytes &gt;= 100</code>       |
| <=       | Less than or equal to  | <code>ip_bytes &lt;= 100</code>       |

Most of the comparison operators should look very familiar and feel pretty straightforward. However, the `IN` operator has two behaviors worth calling out:

- The values in the list must all be of the same type
- The values in the list will all be treated as exact matches
  - Fuzzy matches in lists are not supported

Also, the absence of a property can be tested by comparing the desired field to the `null` keyword.

```
// Returns HTTP requests that did not receive a response
http:status_code == null
```

## Logical operators

Logical operators are used to chain clauses together to form a more complex query.

| Operator | Description   | Example                                     |
|----------|---|---|
| AND      | Both clauses must be satisfied                        | <code>ip = 8.8.8.8 AND port = 53</code>     |
| OR       | Only one clause must be satisfied                     | <code>ip = 8.8.8.8 OR port = 53</code>      |
| NOT      | The inverse must be true (applied to other operators) | <code>ip NOT IN (10.0.0.10, 8.8.8.8)</code> |

Logical operators allow us to chain multiple clause together. However, in the case of `AND`, all field comparisons must apply, which means all event-types involved must support all fields referenced. For example, the following query is illegal because `flow` events don't have a `qtype_name` field and `dns` events don't have a `service` field. In other words, no single event can have both a `flow`-specific field and a `dns`-specific field.

```
// invalid no single event can be both FLOW and DNS
dns:qtype_name = 'A' AND flow:service = 'dns'
```

The above example does not apply to the `OR` operator because a single event could be either a `dns` event or a `flow` event.

```
// This is ok, because a single event could match just one clause
```

```
dns:qtype_name = 'A' OR flow:service = 'dns'
```

## Exclude operators

The 'exclude' operator, for example, A exclude B, provides relative complement filtering that allows all items matching a criteria to be excluded from the result set.

For example, "event\_type = 'flow' and ip != 10.30.0.3" may return an event with src.ip = 10.30.0.1 and dst.ip = 10.30.0.3 because src.ip satisfies the constraint that the event has an ip field that is not 10.30.0.3. This may not be the desired intention. In comparison, "event\_type = 'flow' exclude ip = 10.30.0.3" would not return the event previously described. It will only return flow events excluding those events that match 'ip = 10.30.0.3'.

### Syntax:

The exclude operator is a low precedence, infix operator with left associativity. For example, with A, B, and X below representing complex expressions:

- A exclude X ## base example of matching everything in A except what matches X
- A and B exclude X ## this is the same as (A and B) exclude X
- A or B exclude X ## this is the same as (A or B) exclude X
- A exclude X and Y ## this is the same as A exclude (X and Y)
- A exclude X or Y ## this is the same as A exclude (X or Y)
- A exclude X exclude Y ## this is the same as (A exclude X) exclude Y which is the same as A exclude (X or Y)
- (A exclude X) and (B exclude Y) ## example of using exclude in a restricted context
- exclude X ## This is a special case and interpreted as \* exclude X

## Pattern operators

Pattern operators allow you to identify strings that contain certain patterns. The `LIKE` operator provides simple fuzzy matching, while the `MATCHES` operator provides access to Regex for more complex pattern matching.

| Operator | Description  | Example                                |
|----------|--|--|
| LIKE     | Fuzzy string matching, % for any 0+ characters, _ for any 1 character) | domain NOT LIKE "%.google.com"         |
| MATCHES  | Regex matching   | domain MATCHES ".*\.(com net org edu)" |

Strings must be provided to pattern operators, meaning the characters must be surrounded by quotes. For the `LIKE` operator, the exact string will be matched if no wildcards exist in the provided string.

## Units

IQL supports units for several numeric fields. Units are optional but can greatly increase readability of queries that use time, size, or distance values. Here are some examples:

```
dst.ip_bytes > 5MB // will convert 5MB to 5242880 bytes
dst.ip_bytes > 5.5mb // will convert 5.5mb to 5767168 bytes
```



Unit labels are case insensitive.

## Supported units

| Name         | Type            | IQL Label |
|--------------|-----------------|-----------|
| bytes        | <i>size</i>     | b         |
| kilobytes    | <i>size</i>     | kb        |
| megabytes    | <i>size</i>     | mb        |
| gigabytes    | <i>size</i>     | gb        |
| terabytes    | <i>size</i>     | tb        |
| petabytes    | <i>size</i>     | pb        |
| miles        | <i>distance</i> | mi        |
| kilometers   | <i>distance</i> | km        |
| nanoseconds  | <i>time</i>     | ns        |
| microseconds | <i>time</i>     | us        |
| milliseconds | <i>time</i>     | ms        |
| seconds      | <i>time</i>     | s         |
| minutes      | <i>time</i>     | m         |
| hours        | <i>time</i>     | h         |
| days         | <i>time</i>     | d         |

## Fields with units

| Fields         | Units   |
|----------------|---------|
| geo_distance   | miles   |
| lease_duration | seconds |
| ip_bytes       | bytes   |
| duration       | seconds |
| total_ip_bytes | bytes   |
| request_len    | bytes   |
| request_len    | bytes   |

| Fields     | Units |
|------------|-------|
| file.bytes | bytes |

## Field reference

This section describes how to use fields including where flexibility exists and the implications of that flexibility.

- [Schema and field references on page 124](#)
- [Event-type expansion on page 124](#)
- [Field expansion on page 125](#)
- [Synthetic fields on page 125](#)

## Schema and field references

Queries are evaluated against the events datastore. Every event type has a set of properties – we refer to them as **fields** – that carry data of a defined primitive type. For instance, every event has a `sensor_id` property that is of type `string` and a `timestamp` property of type `timestamp`. The full schema for all available event types and their properties is available within the Event Types page.

All queries consist fundamentally of matching an event field against a value; for instance, "Show me all events for which the destination IP is 8.8.8.8." However, there is some room for flexibility. Do you really want *all* event types, or is there one in particular you're interested. Do you really want to restrict results to cases where 8.8.8.8 is the *destination* IP address, or would any involvement of that IP address be interesting?

Each field involved in a query must be resolved to a specific field of a specific event type. A fully-specified field is of the format `event-type:field`; for instance, `flow:sensor_id` and `dns:dst.geo.country` are both fully specified. For a field that's not fully specified, either by omitting the event type or part of the field, the system will expand the field to include all fully-qualified fields that fit the ambiguity.

The next two subsections will show how these expansions work and what their implications are.

## Event-type expansion

A field without a specified event type will infer all valid event types. For example, `dns` and `flow` events both have a `proto` field, so a query containing just `proto` without an event-type prefix will expand to include both event types. Effectively, the query on the first line below is rewritten by the query engine on the backend to the query on the second line.

```
// original query
proto = 'udp'

// rewrite produced by the query engine on the backend
dns:proto = 'udp' OR flow:proto = 'udp'
```

If a field only belongs to one event type, then the event type does not need to be specified since the results would be the same. For example, the `qtype_name` field is unique to the `dns` event type, so only one event type can be inferred. This means that the two queries below are equivalent.

```
// original query
qtype_name = 'A'
// the rewrite is equivalent
dns:qtype_name = 'A'
```

## Field expansion

Some fields hold values of a structural type (Event Type and Fields), meaning they contain subfields that must be referenced. To make this clear, let's use the `src` field as an example. The `src` field is of the type *ip-object*, i.e. a JSON structure. Looking at the following code block, we couldn't compare `src` to an IP address because we'd have to specify the entire JSON structure for them to match on structure. Instead, we must compare the `ip` subfield to an IP address.

```
// invalid because src is type ip-object and we're comparing it to an ip
src = 10.0.0.10
// valid because src.ip is type ip and we're comparing it to an ip
src.ip = 10.0.0.10
```

If a subfield is used without the parent field, the query will be expanded to include all valid parent fields. For instance, the subfield `ip` could expand to `dst.ip`, `src.ip`, and a number of others. The block below shows the complete expansion for the `ip` field in a `dns` event.

```
// original query
dns:ip = 10.0.0.10
// rewritten to expand the unspecified parent field
dns:src.ip = 10.0.0.10 OR dns:dst.ip = 10.0.0.10 OR dns:answers.ip = 10.0.0.10
```

Event-type and field expansion can be applied to the same query. For example, if we simply specified the `ip` field, the query engine would expand to all possible parent fields in all possible event types.

```
// original query
ip = 10.0.0.10
// complete expansion of event type and parent field (truncated)
dns:src.ip = '10.0.0.10' OR dns:dst.ip = '10.0.0.10' OR dns:answers.ip = 10.0.0.10 OR
flow:src.ip = '10.0.0.10' OR flow:dst.ip = '10.0.0.10'
```

## Synthetic fields

A **synthetic field** is a field that doesn't exist in an event record, i.e. it isn't static. Synthetic fields are dynamically evaluated and converted into static values before your IQL query is run against the event data store. This enables more robust capabilities that aren't possible with a simple query of static values.

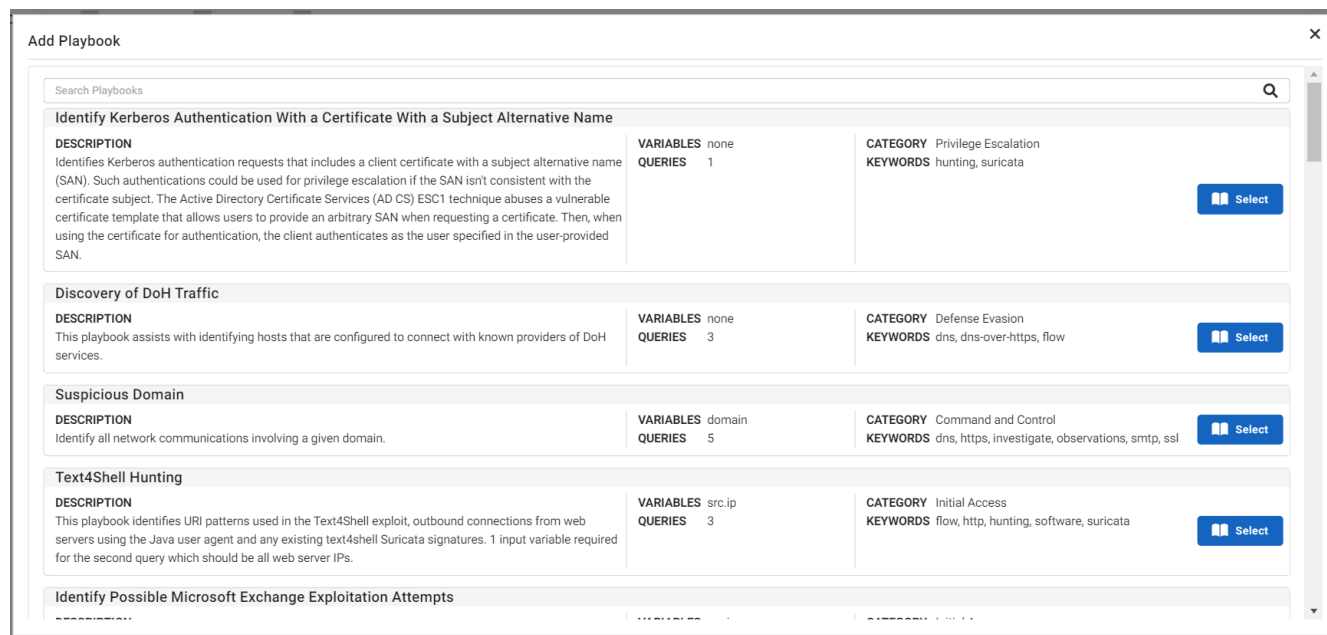
Synthetic fields begin with a `$`. The example query below demonstrates the `$device` synthetic field, which enables a user to search for a source or destination device by hostname or MAC address instead of just the observed IP address.

The hostname is evaluated behind the scenes to produce a large array of IP addresses and valid time ranges, which are then used to query the event data store.

```
src.$device.hostname = 'FinanceWks008' and dst.internal = false
```

## Playbooks

*Playbooks* are queries created by FortiGuard Labs to help you quickly retrieve details in an investigations. You can use a *playbook* to create a new investigation or add a *playbook* to an existing investigation. You can also run a *playbook* of events.

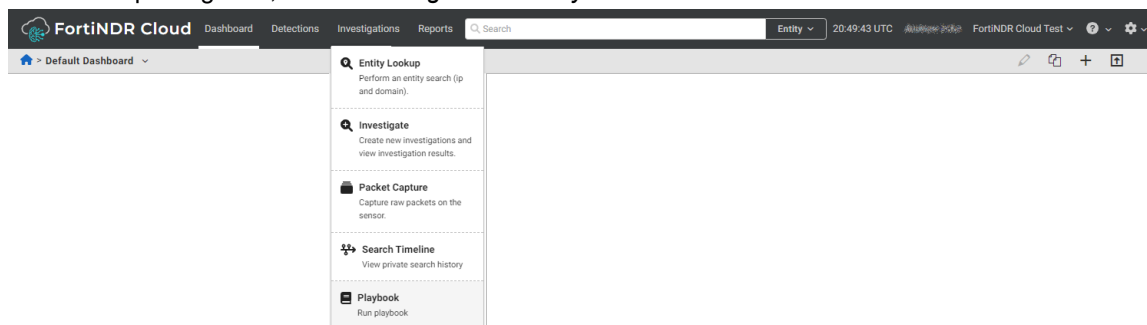


## Running a playbook

Use the navigation menu to open a *playbook* and create a new investigation, or add it to an existing investigation.

**To quickly run a *playbook*:**

1. From the top navigation, select *Investigations > Playbook*.



2. To select a playbook click the playbook name or click *Select*.
3. Configure the playbook settings:

|                                      |   |
|--------------------------------------|---|
| <b>Date range</b>                    | Use the date picker to configure the date range.  |
| <b>Enable Facets</b>                 | Select to return the panel that allows narrowing the search. This may make the query longer to complete. For more information, see <a href="#">Facet Search on page 103</a> .   |
| <b>Variables</b>                     | Enter the required variable(s) for the queries. Multiple variables are supported.<br>Values can be entered either as: <ul style="list-style-type: none"> <li>• Individual items, followed by the tab or enter key. The value appears as a pill that can then be deleted, if required.</li> <li>• <i>Bulk indicator</i> icon. This brings up an entry screen. Pasting the text is supported. After pressing the button, FortiNDR Cloud extracts the applicable indicators from the text and adds them as variables. You can also delete the unneeded variables.</li> </ul> |
| <b>Create a New Investigation</b>    | Select this option to create a new investigation. Enter the <i>Investigation Name</i> and <i>Description</i> .<br>The default name for new investigations is the first and last name of the user creating the investigation as well as a date stamp of when the investigation was created.  |
| <b>Add to Existing Investigation</b> | From the <i>Choose Investigation</i> dropdown, select an investigation.   |

4. Click *Run Playbook*.

## Adding a playbook to an investigation

### To add a playbook to an investigation:

1. Go to *Investigations > Investigate*.
2. Open the investigation you want to add a playbook to.
3. Click the *Add Playbook* button.. Alternatively, click on Add menu (+) in the top-right corner of the page and select *Add Playbook*. The Playbook Library opens.
4. Click *Select* to select a playbook from the library or click the playbook name.
5. Configure the playbook settings.

|                      |   |
|----------------------|---|
| <b>Date range</b>    | Use the date picker to configure the date range.  |
| <b>Enable Facets</b> | Select to return the panel that allows narrowing the search. This may make the query longer to complete. For more information, see <a href="#">Facet Search on page 103</a> .   |
| <b>Variables</b>     | Enter the required variable(s) for the queries. Multiple variables are supported.<br>Values can be entered either as: <ul style="list-style-type: none"> <li>• Individual items, followed by the tab or enter key. The value appears as a pill that can then be deleted, if required.</li> <li>• <i>Bulk indicator</i> icon. This brings up an entry screen. Pasting the text is supported. After pressing the button, FortiNDR Cloud extracts the applicable indicators from the text and adds them as variables. You can also delete the unneeded variables.</li> </ul> |

**Create a New Investigation** Select this option to create a new investigation. Enter the *Investigation Name* and *Description*. The default name for new investigations is the first and last name of the user creating the investigation as well as a date stamp of when the investigation was created.

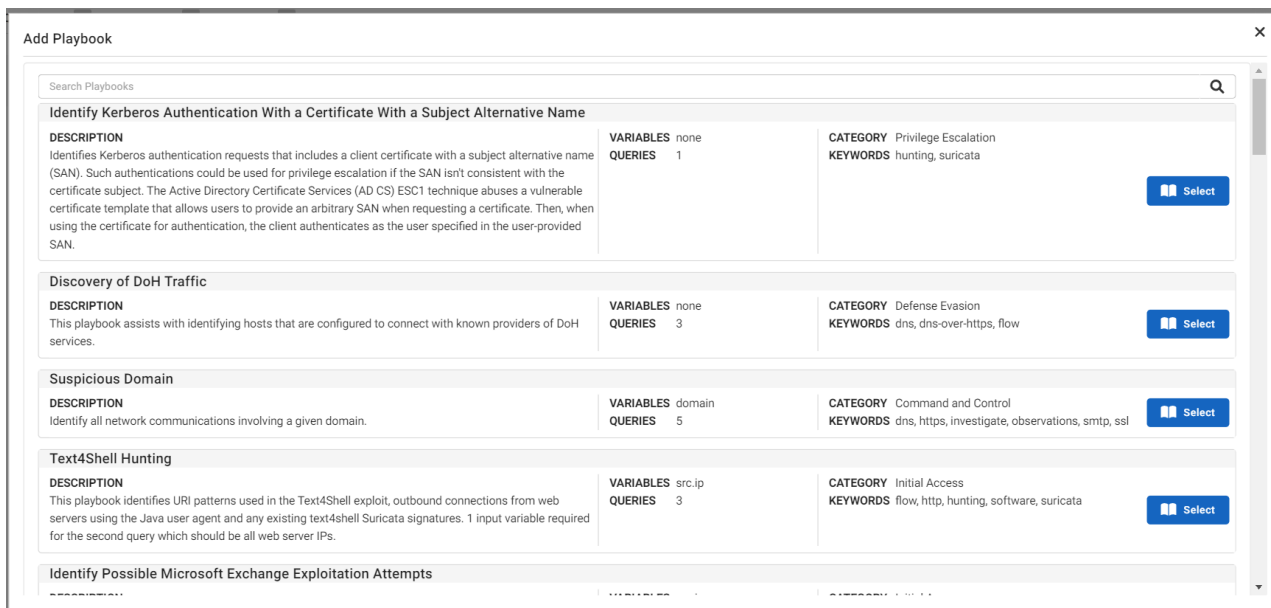
**Add to Existing Investigation** From the *Choose Investigation* dropdown, select an investigation.

6. Click *Run Playbook*.

## Running a playbook of event records

To run a playbook of event records:

1. Go to *Investigations > Investigate*.
2. Select an investigation from the list.
3. Click *View Results* to view the investigation results.
4. Right click on an entity to open the context menu and select *Playbooks*.



5. Select a playbook from the list. If the event record has matching variables in the playbook, then the variables will be populated with values from the event record.

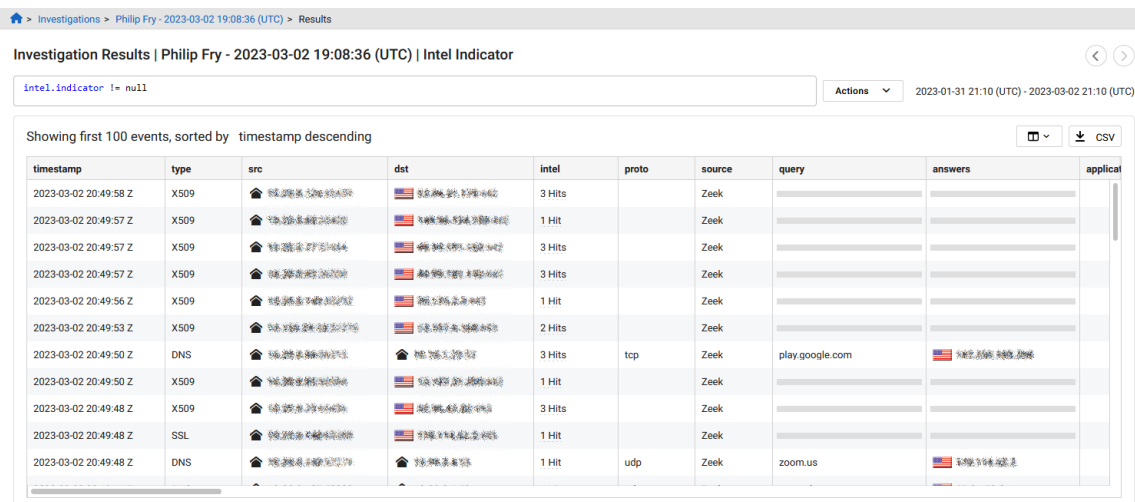




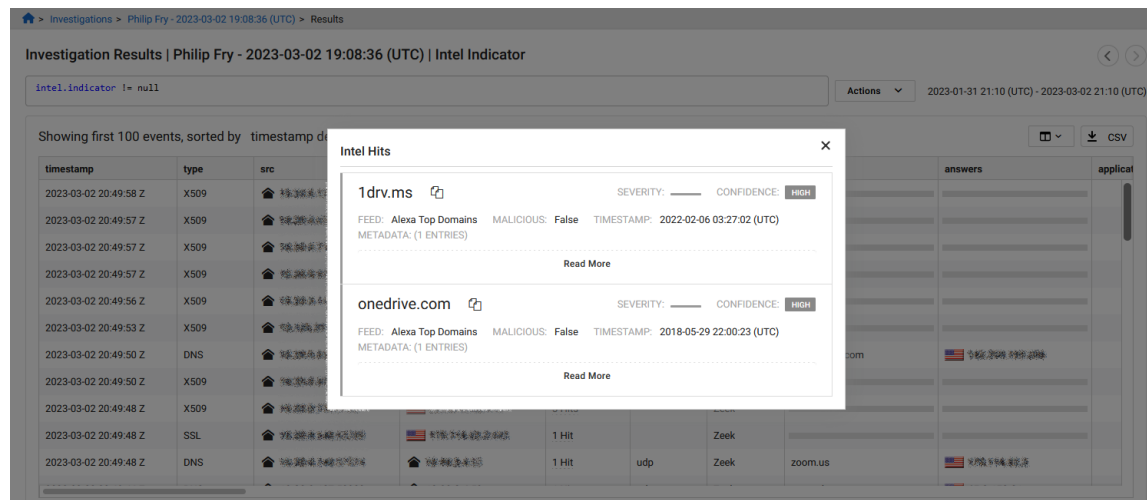
## Example query:

The following query is a simple way to determine whether or not network traffic has matched with threat intelligence data in your network. When the results load, you will notice the `intel` column shows whether or not an event has a match against a threat intelligence source.

```
// show events that have at least one matched intel record
intel.indicator != null
```



Click the number of *hits* in the *Intel* column to view the matched *intel* records.



## Search for intel

The `intel` field is an array of *intel-objects*, meaning there could be multiple records for a given event. When a query is applied to an event with multiple intel records, the values for each field are flattened into individual arrays before the query logic is applied to the values.

The following table lists the fields contain in *intel-objects*:

| Field          | Type      | Description   | Example   |
|----------------|-----------|---|---|
| confidence     | String    | The overall confidence rating of the intel source           | high  |
| feed           | String    | The name of the intel source                                | Sinkholes   |
| indicator      | String    | The matched entity  | 131.253.18.12   |
| indicator_type | String    | The entity type   | ip_address  |
| is_malicious   | Boolean   | Indicates whether the indicator is believed to be malicious | false   |
| meta           | String    | A JSON string of all metadata provided by the intel source  | {"description": "Observed C2 Activity", "references": ["Fortinet FortiGuard Labs"]} |
| severity       | String    | The overall severity rating of the intel source             | high  |
| timestamp      | Timestamp | The creation time of the intel record                       | 2019-01-01T00:00:00.000Z  |

## Example search for intel

In this example, we will create two queries to search for the following events:

- **Event 1:** [{confidence: high, severity: low}, {confidence: low, severity: high}]
- **Event 2:** [{confidence: high, severity: high}, {confidence: low, severity: low}]

### Example 1:

In this example we will use a query to compare an array of records in *Event 1* and *Event 2*.

#### Query string:

```
intel.confidence = high & intel.severity = high
```

#### What the query will do:

1. The two records are flattened into arrays of values for each field, so the query logic is applied to all values all at once and not to records individually.
2. The query is compared to the array of records in *Event 1* and *Event 2*.

#### Response:

This query will return Event 1 and 2 because at least one inner object contains `confidence=high` and at least one inner object contains `severity=high`.

- Event 1: confidence =[high,low] and severity = [high,low]
- Event 2: confidence =[high,high] and severity = [high,low]

### Example 2:

In this example, we will create a query to match individual objects of a nested field (such as intel, path, files, etc.).

#### Query string:

```
intel {confidence=high & severity=high}
```

#### Response:

This query will only return Event 2 because at least one of the objects in the event meets both criteria.

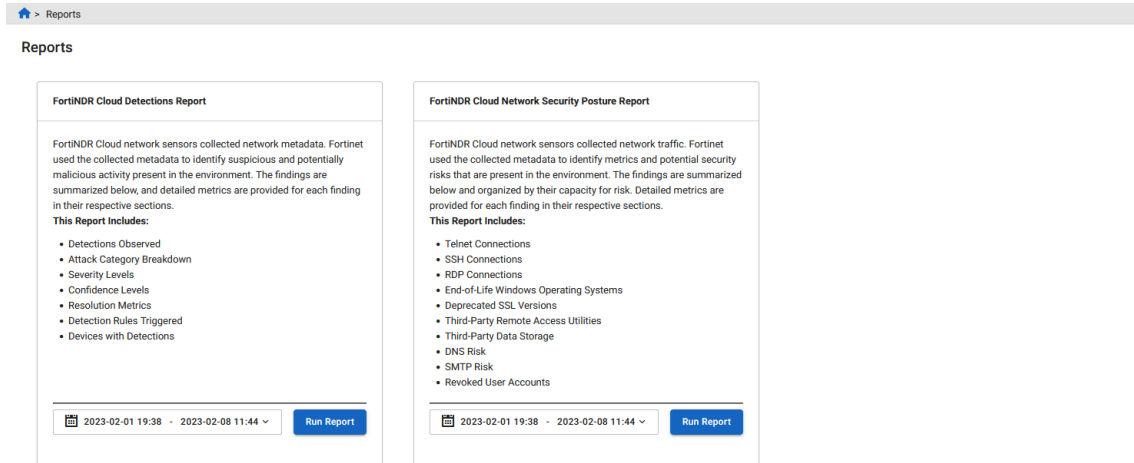
- Event 2: confidence =[high,high] and severity = [low,low]

# Reports

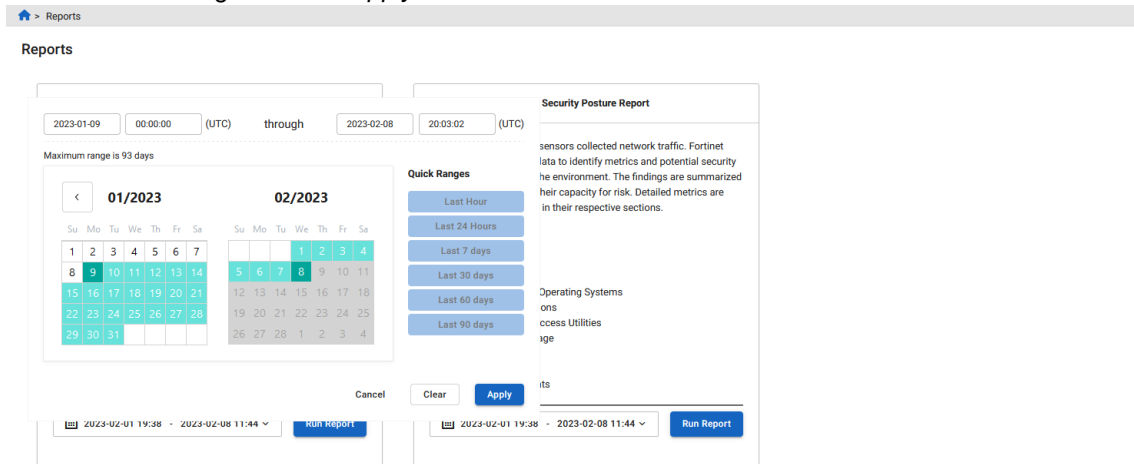
You can create a custom report for a specified date range to view in the browser.

## To generate a report:

1. From the top navigation, select *Reports*.



2. Use the calendar drop-down to select the date range for the report.
3. Select the date range and click *Apply*.



4. Click *Run Report*.

The browser will transition from the template list to the report page while retrieving data to complete the report. Each section will update individually as data is retrieved. Spinners will appear while data is being loaded. Sections will appear as data is ready.

FortiNDR Cloud Detections Report

Executive Summary

FortiNDR Cloud network sensors collected network metadata. Fortinet used the collected metadata to identify suspicious and potentially malicious activity present in the environment. The findings are summarized below, and detailed metrics are provided for each finding in their respective sections.

Detection Statistics

|                  |                         |                     |
|------------------|-------------------------|---------------------|
| Total Detections | Devices with Detections | Resolved Detections |
| 142              | 29                      | 70                  |

Resolution Metrics

|                            |                      |                 |
|----------------------------|----------------------|-----------------|
| Mean Time to Detect (MTTD) | Mean Time to Respond | Mean Dwell Time |
| 9m                         | 9d 23h               | 9d 23h          |

Detections Observed

OVERVIEW

The Detections feature is the alerting mechanism for the FortiNDR Cloud solution, which is designed to enable you to quickly identify and respond to suspicious or known-bad activity in your network. Detection rules are organized into the following high-level categories: Attack, Posture, and PUJ.

**142**  
Total Detections

**29**  
Devices with Detections

FortiNDR Cloud Network Security Posture Report

Executive Summary

FortiNDR Cloud network sensors collected network traffic. Fortinet used the collected metadata to identify metrics and potential security risks that are present in the environment. The findings are summarized below and organized by their capacity for risk. Detailed metrics are provided for each finding in their respective sections.

Findings

|  |           |            |
|--|-----------|------------|
| Total Hosts Receiving Telnet Connections                         | 8 Hosts   | HIGH       |
| Total Internal Hosts Receiving SSH Connections                   | 84 Hosts  | HIGH       |
| Total Internal Hosts Receiving RDP Connections                   | 2 Hosts   | HIGH       |
| Hosts Potentially Running EOL Versions of Windows                | 1 Hosts   | HIGH       |
| Total Internal Hosts Serving SSLv2, SSLv3, or TLSv1.0            | 13 Hosts  | MODERATE   |
| Total Hosts Communicating with Remote Access Services via HTTP   | Hosts     | UNOBSERVED |
| Total Hosts Communicating with Remote Access Services via SSL    | Hosts     | UNOBSERVED |
| Total Hosts Using Remote Storage Services via SSL                | Hosts     | UNOBSERVED |
| Total Hosts Using Remote Storage Services via HTTP               | Hosts     | UNOBSERVED |
| Internal Hosts Directly Using External DNS Servers               | 119 Hosts | LOW        |
| Internal Hosts Directly Communicating with External SMTP Servers | 1 Hosts   | LOW        |
| Total Revoked Accounts with Authentication Attempts              | 1 Hosts   | LOW        |

HIGH

The observed activity indicates an ongoing security issue or significantly decreases the security posture of the organization's environment.

MODERATE

The observed activity could lead to future security issues.

LOW

The observed activity may not pose an immediate risk but does not follow best practices

Telnet Connections

RATING

HIGH

1

Hosts Receiving Inbound External Telnet Connections

OVERVIEW

Telnet is a protocol that provides remote access to a command-line interface (usually of an operating system).

TOT

# Settings

You can apply global settings FortiNDR Cloud by clicking on the gear in the top-right corner of the portal.


## Profile settings

Use *Profile Settings* to configure your profiles such as your account and configure authentication.

### My profile

|                            |   |
|----------------------------|---|
| <b>User Information</b>    |   |
| <b>User Email</b>          | The email the user logs into the application with.  |
| <b>User Name</b>           | The user's first and last name.   |
| <b>User UUID</b>           | The user's unique ID.   |
| <b>User MFA</b>            | Indicates if Multifactor Authentication is disabled or enabled.   |
| <b>Account Information</b> |   |
| <b>Account Name</b>        | The name of the account the user belongs to.  |
| <b>Account UUID</b>        | The account's unique ID.<br>The Account UUID is useful when interacting with the APIs. Most APIs allow you to specify an account UUID to pull data for; this is equivalent to setting the Account Selector to a specific account. If you do not specify an account UUID, you receive data from all accounts you have access to. |

### Authentication

|                                    |   |
|------------------------------------|---|
| <b>Password</b>                    | Click <a href="#">Change my password</a> to update your FortiNDR Cloud password.<br>Passwords must be a minimum of eight characters and are valid for 180 days. FortiNDR Cloud will notify you when your password is about to expire. If you attempt to log in after your password has expired, you will be prompted to create a new password.                      |
| <b>Multi-Factor Authentication</b> | Click <a href="#">Enable MFA</a> to enter a token each time you log into FortiNDR Cloud.<br><hr/>  Multi-Factor Authentication requires a Time-based one-time password (TOTP) such as FortiToken.<br>You will be required to configure an MFA token as soon as you log in. <hr/> |

## Token

### Permanent Token

Click *Create New Token* to create permanent authentication tokens for authenticating API calls. These tokens never expire, and remain valid until revoked.

## Manage subscriptions

Receive an email notification when a rule triggers a detection. Subscriptions are configured and applied on a per-user basis using the email address tied to a user's account. If you are logging in for the first time or have never updated your subscriptions, you will see the Default Subscription created for every user.

You can manage subscriptions from the application settings or the detections settings menu.

### To create a subscription:

1. Go to *Detections*.
2. In the toolbar, click the gear icon menu and click *Manage Subscriptions*. The *Subscriptions* page opens.
3. Click the *Create subscription* button at the top right-side of the page. A blank subscription is displayed.



4. Configure the subscription:

| Subscription Name | Enter a name for the subscription.   |   |             |          |             |   |  |                 |  |  |            |                              |   |
|-------------------|--|---|-------------|----------|-------------|---|--|-----------------|--|--|------------|------------------------------|---|
| Severities        | Select one of the following:   |   |             |          |             |   |  |                 |  |  |            |                              |   |
|                   | <table border="1"> <thead> <tr> <th>Severity</th> <th>Description</th> <th>Examples</th> </tr> </thead> <tbody> <tr> <td><b>High</b></td> <td>Significant to fair impact with the potential to spread or escalate</td> <td>Malicious code execution, C2 communications, lateral movement, data exfiltration</td> </tr> <tr> <td><b>Moderate</b></td> <td>Fair impact with minimal potential to spread or escalate</td> <td>Activity that could indicate malicious intent, untargeted attacks with unknown success, data leakage, subversion of security or monitoring tools</td> </tr> <tr> <td><b>Low</b></td> <td>Little to no impact expected</td> <td>Potentially unauthorized software, devices, or resource use, untargeted adware or spyware, compromise of a personal device or device on an untrusted network, insecure configurations</td> </tr> </tbody> </table> | Severity  | Description | Examples | <b>High</b> | Significant to fair impact with the potential to spread or escalate | Malicious code execution, C2 communications, lateral movement, data exfiltration | <b>Moderate</b> | Fair impact with minimal potential to spread or escalate | Activity that could indicate malicious intent, untargeted attacks with unknown success, data leakage, subversion of security or monitoring tools | <b>Low</b> | Little to no impact expected | Potentially unauthorized software, devices, or resource use, untargeted adware or spyware, compromise of a personal device or device on an untrusted network, insecure configurations |
| Severity          | Description  | Examples  |             |          |             |   |  |                 |  |  |            |                              |   |
| <b>High</b>       | Significant to fair impact with the potential to spread or escalate  | Malicious code execution, C2 communications, lateral movement, data exfiltration  |             |          |             |   |  |                 |  |  |            |                              |   |
| <b>Moderate</b>   | Fair impact with minimal potential to spread or escalate   | Activity that could indicate malicious intent, untargeted attacks with unknown success, data leakage, subversion of security or monitoring tools                                      |             |          |             |   |  |                 |  |  |            |                              |   |
| <b>Low</b>        | Little to no impact expected   | Potentially unauthorized software, devices, or resource use, untargeted adware or spyware, compromise of a personal device or device on an untrusted network, insecure configurations |             |          |             |   |  |                 |  |  |            |                              |   |
| Confidences       | Select one of the following:   |   |             |          |             |   |  |                 |  |  |            |                              |   |



|            | Confidence   | Minimum True-Positive Rate |
|------------|--|----------------------------|
|            | High   | 90%                        |
|            | Moderate   | 75%                        |
|            | Low  | 50%                        |
| Categories | Select a category from the list. For information, see <a href="#">Detections &gt; Rule Categories</a> .  |                            |
| Account    | Select the account the rule belongs to.  |                            |
| Email Type | <ul style="list-style-type: none"> <li>• <i>Notification</i>: Sends an email for each individual rule that becomes active.</li> <li>• <i>Digest</i>: Sends you a single email each day at the specified time (default 08:00 Eastern) summarizing rules that became active and/or were resolved during the previous day.</li> </ul> |                            |

5. Click **Save**.



#### To delete a subscription:

1. Go to *Detections*.
2. In the toolbar, click the gear icon menu and click *Manage Subscriptions*. The *Subscriptions* page opens.
3. Click the *Actions* menu at the left side of the rule and select *Edit Subscription*.
4. Click *Delete*.



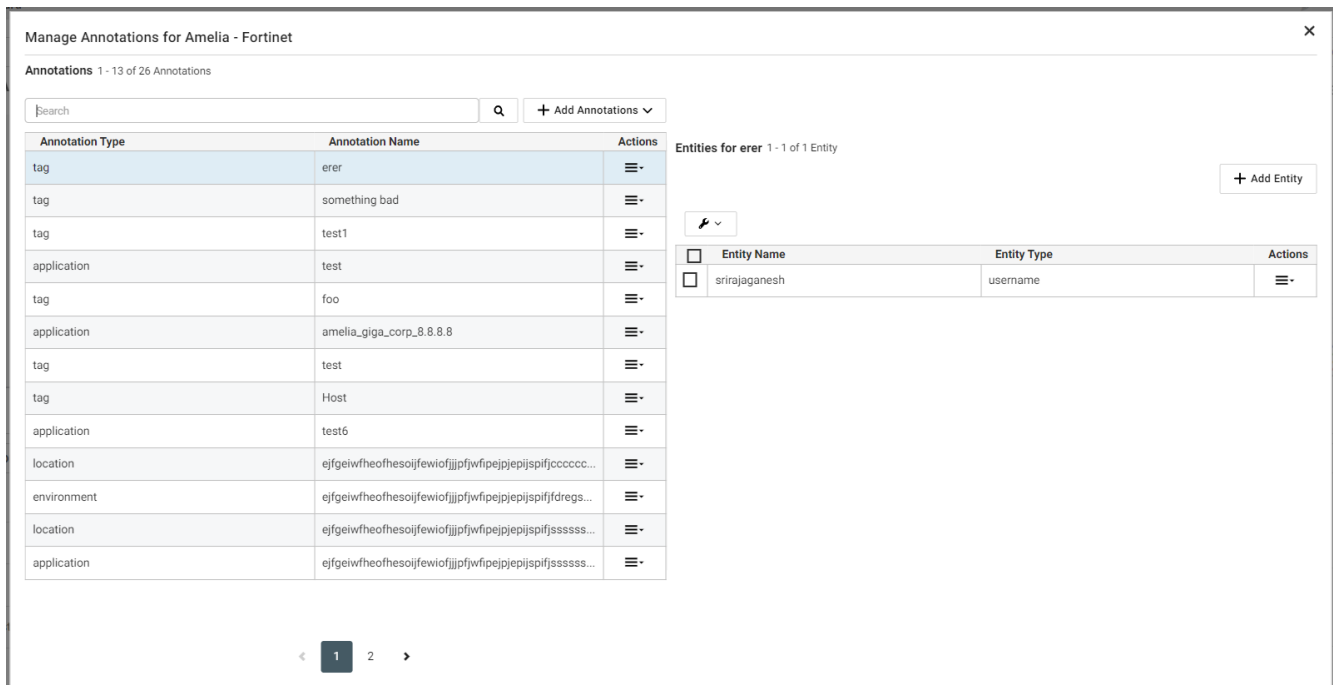
#### To disable a subscription:

1. Go to *Detections*.
2. In the toolbar, click the gear icon menu and click *Manage Subscriptions*. The *Subscriptions* page opens.
3. Click *Delete*.



## Manage Annotations

*Manage Annotations* settings allow you to view and edit all your annotations in one place.



**To create an annotation:**

1. Click *Add Annotations > Create Annotation*.
2. Configure the annotation settings:

|                                   |   |
|-----------------------------------|---|
| <b>Select an annotation type:</b> | Select <i>Application, Environment, Location, Owner, Role</i> or <i>Tag</i> . |
| <b>Enter an annotation name</b>   | Enter a name for the annotation.  |
| <b>Enter a description</b>        | Enter the annotation.   |

3. Click *Save*.

**To add annotations with a CSV file:**

1. Create the CSV file. The file must contain the following : *annotation type, annotation name, description, entity, entity\_type*.

|   | A           | B          | C                 | D       | E           |
|---|-------------|------------|-------------------|---------|-------------|
| 1 | location    | USA        | us head           | 1.1.1.1 | ip          |
| 2 | environment | Prod       | prod              | 1.1.1.1 | ip          |
| 3 | owner       | test owner | owner description | test    | application |
| 4 | tag         | test tag   |                   | 1.1.1.1 | ip          |

2. Click *Add Annotations > Upload CSV*.
3. Upload the CSV file.
4. Click *Save*.

**To edit an annotation:**

1. Click the gear icon in the top-right corner of the application.
2. Click *Manage Annotations*.



3. Click the *Actions* menu at the right side of the annotation and select *Edit Annotation*.
4. Update the annotation and click *Save*.

**To delete an annotation:**

1. Click the gear icon in the top-right corner of the application.
2. Click *Manage Annotations*.



3. Click the *Actions* menu at the right side of the annotation and select *Remove Annotation*.
4. Click *Confirm*.

**To add an entity:**

1. Click the gear icon in the top-right corner of the application.
2. Click *Manage Annotations*.
3. Enter one or more entities(IP Address, CIDR, domain or username) separated by comma, space, or return.
4. Click *Save*.

**To bulk remove entities:**

1. Click the gear icon in the top-right corner of the application.
2. Click *Manage Annotations*.
3. Click *Remove bulk entities*.



4. Click *Confirm*.

## Sensors

The *Sensors* page shows the sensors deployed in your account, both in the aggregate and individually. Use this page to generate provisioning codes, check the status of individual sensors, and view telemetry data.

To access to the *Sensors* page, click the gear icon at the top-right of the page and select *Sensors*.

| SENSOR ID | STATUS | VERSION | LABELS | LOCATION     | EPS (7 DAY AVERAGE) | BITS/S (7 DAY AVERAGE) | TYPE |
|-----------|--------|---------|--------|--------------|---------------------|------------------------|------|
| tma1      | online | 1.11.0  |        | Sunnyvale CA | 13 EPS              | 972.943 Kb/s           | ESXi |

|                                |   |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
|--------------------------------|---|---------------|---|----------------|--|---------------------|--|-----------------------|--|--------------------------------|--|------------------------------|---|-----------------|---|
| <b>Sensor ID</b>               | Click the Sensor ID to view the sensor <i>Status</i> , <i>Telemetry</i> and <i>Settings</i> pages. For information, see <a href="#">Sensor status on page 141</a>   |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
| <b>Status</b>                  | <p>The sensor connection status.</p> <table border="1"> <tr> <td><b>Online</b></td> <td>Sensor is connected to FortiNDR Cloud within last hour.</td> </tr> <tr> <td><b>Offline</b></td> <td>No telemetry data received by the sensor for at least an hour.</td> </tr> <tr> <td><b>Provisioning</b></td> <td>Provisioning code has been created and made initial connection but provisioning process is not complete.</td> </tr> <tr> <td><b>Decommissioned</b></td> <td>Sensor has been factory reset (only applicable for 1.12 or above).</td> </tr> <tr> <td><b>Decommissioned (legacy)</b></td> <td>A sensor earlier than 1.12 has been marked as decommissioned and has not sent any additional data. If sensor sends data to FortiNDR Cloud, status will change to <i>Online</i>.</td> </tr> <tr> <td><b>Decommissioned (auto)</b></td> <td>A sensor 1.12 or later has been marked as decommissioned, but has not communicated with FortiNDR Cloud in the last 7 days. If the sensor later connects to FortiNDR Cloud, it should factory reset itself and switch to <i>Decommissioned</i> status.</td> </tr> <tr> <td><b>Shutdown</b></td> <td>A Zscaler virtual sensor is no longer active.</td> </tr> </table> <p>All other statuses are written by the sensor itself.</p> | <b>Online</b> | Sensor is connected to FortiNDR Cloud within last hour. | <b>Offline</b> | No telemetry data received by the sensor for at least an hour. | <b>Provisioning</b> | Provisioning code has been created and made initial connection but provisioning process is not complete. | <b>Decommissioned</b> | Sensor has been factory reset (only applicable for 1.12 or above). | <b>Decommissioned (legacy)</b> | A sensor earlier than 1.12 has been marked as decommissioned and has not sent any additional data. If sensor sends data to FortiNDR Cloud, status will change to <i>Online</i> . | <b>Decommissioned (auto)</b> | A sensor 1.12 or later has been marked as decommissioned, but has not communicated with FortiNDR Cloud in the last 7 days. If the sensor later connects to FortiNDR Cloud, it should factory reset itself and switch to <i>Decommissioned</i> status. | <b>Shutdown</b> | A Zscaler virtual sensor is no longer active. |
| <b>Online</b>                  | Sensor is connected to FortiNDR Cloud within last hour.   |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
| <b>Offline</b>                 | No telemetry data received by the sensor for at least an hour.  |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
| <b>Provisioning</b>            | Provisioning code has been created and made initial connection but provisioning process is not complete.  |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
| <b>Decommissioned</b>          | Sensor has been factory reset (only applicable for 1.12 or above).  |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
| <b>Decommissioned (legacy)</b> | A sensor earlier than 1.12 has been marked as decommissioned and has not sent any additional data. If sensor sends data to FortiNDR Cloud, status will change to <i>Online</i> .  |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
| <b>Decommissioned (auto)</b>   | A sensor 1.12 or later has been marked as decommissioned, but has not communicated with FortiNDR Cloud in the last 7 days. If the sensor later connects to FortiNDR Cloud, it should factory reset itself and switch to <i>Decommissioned</i> status.   |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
| <b>Shutdown</b>                | A Zscaler virtual sensor is no longer active.   |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
| <b>Version</b>                 | The sensor version. <i>Unknown</i> is displayed when there is no data for the version.  |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
| <b>Labels</b>                  | Annotations that are applied to the sensor. See, <a href="#">Manage Annotations on page 137</a>   |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
| <b>Location</b>                | The sensor location.  |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
| <b>EPS (7 Day Average)</b>     | The average throughput over last 7 days as Events Per Second  |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
| <b>BITS/S (7 Day Average)</b>  | The average throughput over last 7 days as Bits Per Second.   |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
| <b>Type</b>                    | The platform the sensor was deployed on.  |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |
| <b>Actions</b>                 | Click to edit the sensor settings. See <a href="#">Sensor settings on page 143</a> .  |               |   |                |  |                     |  |                       |  |                                |  |                              |   |                 |   |

### To filter the Sensors page:

1. In the toolbar, click the filter icon.



2. Click the *Status* dropdown to filter by status. The default filter is any status that is not *Decommissioned*. The filter only displays the available statuses.
3. Click the *Type* dropdown to filter the page by the sensor type.

## Sensor status

To view the status page for a sensor, click the sensor ID in *Sensors* page. The *Status* tab shows information regarding the physical deployment of the sensor.

### Connection Status

The *Connection Status* section displays the state of the sensor's connectivity to FortiNDR Cloud's infrastructure and the IP address of the sensor's management interface. The *Interfaces* section lists each network interface on the sensor. The sensor's management interface will be indicated with the string *mgmt*. A green interface indicates that a cable is connected, while gray indicates that a cable is not connected. Additionally, you can click on the interface label to view its MAC address.

Sensors for **gssso847** ✖ Offline

| CREATED             | LOCATION | EPS (7 DAY AVERAGE) | BITS/S (7 DAY AVERAGE) | TYPE |
|---------------------|----------|---------------------|------------------------|------|
| 2024-01-16 22:00:30 |          | 0 eps               | 0 b/s                  | ESXI |

- Status
- Telemetry
- Settings

#### Connection Status

Status: ⊘ offline

Serial Number: VMware-56 4d 2e 53 59 ca 13 26-38 eb 73 32 f2 58 b2 6e

Management IP: [REDACTED]

#### Interfaces

**ens192**

mgmt

0 b/s

**ens224**

0 b/s

#### Hardware

Processor(s): Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz

Number of Cores: 8

Total Memory: 15.638 GB

Total Disk Space: 67.944 GB

#### Software

Operating System: Debian GNU/Linux 10 (buster)

ZEEK Version: 5.0.10

Suricata Version: 6.0.12 RELEASE

Sensor Version: 1.12.0

#### Sensor History

34 record(s), sorted by Timestamp descending

| Timestamp | Action | User Account Name | User Name | Comment |
|-----------|--------|-------------------|-----------|---------|
|           |        |                   |           |         |

The following table details the naming convention for interfaces on FortiNDR Cloud sensors.

| Label | Sensor Type | Interface Type | Purpose    | Max Bandwidth |
|-------|-------------|----------------|------------|---------------|
| em4   | Physical    | Ethernet       | Management | 1 Gb/s        |
| em3   | Physical    | Ethernet       | Monitoring | 1 Gb/s        |
| em2   | Physical    | Ethernet       | Monitoring | 10 Gb/s       |
| em1   | Physical    | Ethernet       | Monitoring | 10 Gb/s       |
| p#p## | Physical    | Fiber          | Monitoring | 10 Gb/s       |
| eth0  | Virtual     | Virtual        | Management | N/A           |
| eth1+ | Virtual     | Virtual        | Monitoring | N/A           |



The *Max Bandwidth* column shows the physical limitation of the interface, not the maximum sustained bandwidth that the sensor can handle.

## Hardware

The Hardware pane displays the sensor *Processor(s)*, *Number of Cores*, *Total Memory* and *Total Disk Space*.

| Hardware          |   |
|-------------------|---|
| Processor(s):     | Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz |
| Number of Cores:  | 8   |
| Total Memory:     | 15.638 GB                                 |
| Total Disk Space: | 67.944 GB                                 |

## Software

The Software pane displays the *Operating System*, *ZEEK Version*, *Suricata Version* and *Sensor Version*.

| Software          |         |
|-------------------|---------|
| Operating System: |         |
| BRO Version:      |         |
| Suricata Version: |         |
| Sensor Version:   | Unknown |

## Sensor History

The *Sensor History* table shows the actions performed (*paused* or *resumed*), the user who initiated the action, well as any comments from the user. The table is sorted in descending order by timestamp. A message appears if there is no history to display.

| Sensor History                               |        |                   |           |         |
|--|--------|-------------------|-----------|---------|
| 34 record(s), sorted by Timestamp descending |        |                   |           |         |
| Timestamp                                    | Action | User Account Name | User Name | Comment |
| 2024-01-27T13:02:01.998983Z                  | pause  |                   |           |         |
| 2024-01-27T12:56:07.131922Z                  | resume |                   |           |         |
| 2024-01-27T12:55:48.642531Z                  | pause  |                   |           |         |
| 2024-01-27T02:07:50.782904Z                  | resume |                   |           |         |
| 2024-01-27T01:46:45.553064Z                  | pause  |                   |           |         |

## Telemetry

The *Telemetry* tab plots measurements of total throughput across the sensor's interfaces in bits per second, and the number of events produced by the sensor. These plots can be found on the *Throughput* and *Events* tabs, respectively. Measurements for both are available in perpetuity. Each plot can be displayed as either a line or bar plot for any time period, and the *Events* plot can be grouped by event type.

The *Telemetry* page also displays observed devices for the sensor on the *Visibility* tab. This data is essentially a slimmed down version of the *Devices* page.

## Settings

The *Settings* tab shows the configurable fields for a sensor. This includes a sensor's location, arbitrary labels (hostname, site/building code, etc.), and whether to enable PCAP.



To modify these settings, contact your Technical Success Manager.



Enabling PCAP has security and privacy complications. Before enabling PCAP, consult with your Technical Success Manager.

For example, networks with data that is subject to regulatory requirements may require certain controls to be in place before enabling this feature. Enabling this feature may also require uploading a public key to encrypt any PCAPs. See, [Account management on page 146](#) or contact Customer Support for more information on public keys.

## Account Telemetry

The Account Telemetry page shows aggregated telemetry data from all sensors in your account.



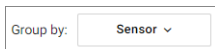
To view the telemetry for each sensor, click the *Telemetry* tab in the *Sensor Status* page. See [Sensor status on page 141](#).

### To view the Account Telemetry page:

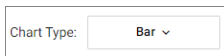
1. Click the gear icon at the top-right of page select *Sensors*.
2. Click the *Telemetry* tab. The *Throughput* page opens.



3. Click *Date Range* to configure the date range using the date picker, or choose a value from the *Quick Ranges* list.
4. To group the events, click the *Group by* drop down and select a value from the list.



5. Click *Chart Type* to switch between *Line* and *Bar* views.




## Sensor settings

Use the sensor *Settings* page to update the sensor location, make annotations and enable or disable Packet Capture. You can also access the sensor settings from the *Actions* menu on the *Sensors* page.

**Requirements:**

- You must have Admin privileges to edit the sensor settings.

**To edit the sensor settings:**

- Click the gear icon at the top-right of page select *Sensors*. The *Sensor* page opens.  

- Click the *Sensor ID*. The sensor *Status* page opens.
- Click the *Settings* tab. The *General* page displays the sensor *Location*, *Labels* and *PCAP* status.
- Click *Edit General Settings* to edit the sensor *Location* and *Labels*.

|                 |  |
|-----------------|--|
| <b>Location</b> | Update the sensor location.  |
| <b>Labels</b>   | Enter keywords about the sensors. To add annotation, type the phrase or keyword and press Tab or Enter.<br>Annotations with an orange background are internal and cannot be edited.<br>Annotations with a blue background can be added or deleted. |

- Click *Edit Features Settings* to enable/disable *Packet Capture*.

|                     |   |
|---------------------|---|
| <b>PCAP Enabled</b> | Enable packet capture. For more information, see <a href="#">Packet Capture on page 107</a> . |
|---------------------|---|

**To edit the settings from the Sensors page:**

- On the *Sensors* page, click the actions menu at the right side of the page and click *Edit*.



- Update the Sensor details and click *Update*.

|                     |  |
|---------------------|--|
| <b>Location</b>     | Update the sensor location.  |
| <b>Annotations</b>  | Enter keywords about the sensors. To add annotation, type the phrase or keyword and press Tab or Enter.<br>Annotations with an orange background are internal and cannot be edited.<br>Annotations with a blue background can be added or deleted. |
| <b>PCAP Enabled</b> | Enable packet capture. For more information, see <a href="#">Packet Capture on page 107</a> .  |

## Device view

FortiNDR Cloud continuously collects data on the devices present in a network. This data is collected on a per sensor basis, since multiple sensors may report the same IP address, either due to re-use of IP space within a single environment, or through traffic from an IP crossing multiple monitoring points.

You can use Device View to:

- Quantify FortiNDR Cloud sensor visibility coverage over time.
- Verify that FortiNDR Cloud sees both internal and external traffic from network devices.



Visible Devices for [redacted]

All Subnets Search  Date

Devices by Subnet (15 Total) Highlight By: External Traffic % View:

3 SUBNETS SEEN BETWEEN 2023-05-03 AND 2023-05-03 View:    CSV

| Subnet     | Device Count | % of Devices with External Traffic | % of Devices with Internal Traffic |
|------------|--------------|------------------------------------|------------------------------------|
| [redacted] | 9            | 88.89%                             | 77.78%                             |
| [redacted] | 3            | 0%                                 | 100%                               |
| [redacted] | 3            | 66.67%                             | 100%                               |

## Viewing visible devices

To view the visible devices:

1. Click the gear icon at the top-right of the page and select *Sensors*.



2. In the toolbar, click *Visible Devices*. The page is organized into three sections:

|                          |                           |  |
|--------------------------|---------------------------|--|
| <b>All Subnets</b>       | <b>Search</b>             | Enter a subnet or prefix to view a specific device.  |
|                          | <b>Date</b>               | Click to open the date picker to view devices within a specif date range.  |
|                          | <b>Additional Filters</b> | Click the filter icon to view devices by sensor and Internal and External traffic directions.  |
| <b>Devices by Subnet</b> | <b>Highlight by</b>       | <p>Select <i>External Traffic %</i> or <i>Internal Traffic %</i> to change the colors in the box-plot chart to show the percentage of assets.</p> <p>Use this view to verify FortiNDR Cloud is seeing both internal (East-West) and external (North-South) traffic on a specific subnet.</p> |
|                          | <b>View</b>               | <ul style="list-style-type: none"> <li>• <i>By Subnet</i>: This the default view.</li> <li>• <i>Over Time</i>: Shows how many devices were seen within the selected subnet over time. This graph is if sensor coverage is experiencing issues or to debug problems with missing</li> </ul>   |

events for a certain time period.

**Box-plot chart**

Click the box-plot chart to drill down into the selected subset of the network.

**# SUBNETS SEEN BETWEEN  
YYYY-MM-DD AND YYYY-  
MM-DD**

Shows either a summary of subnets or a list of discrete devices. This table is useful for reviewing the traffic on a per device basis.

## Account management

Use the *Account Management* page to create new users and manage global settings for your account. You must have Admin privileges for one or more accounts to view the *Account Management* page.

### To view the Account Management page:

Click the gear icon at the top-right of the page and select *Account Management*.

- If you have access to only one account, you will see the *Account Management* page for your account
- If you have Admin privileges for more than one account, you will see the *Account Inventory* page. From there, click an account to view its *Account Management* page.

The top of the page will display descriptive parameters for the account, namely the account's UUID and sensor code, as well as the number of users and sensors provisioned in the account. The rest of the page is organized into the following sections:

The *Account Management* page contains the following tabs:

|                        |  |
|------------------------|--|
| <b>Users</b>           | Create new users and assign roles.   |
| <b>Subnets</b>         | <p>Lists all internal IP address ranges for the account. This list will always include the ranges defined in RFC 1918, link local addresses (169.254.0.0/16), and multicast addresses (224.0.0.0/4).</p> <p>We recommend adding a public IP space owned by your organization, such as post-NAT, egress, or externally-accessible IP addresses, to this list. Doing so better characterizes the directionality of your network's traffic.</p> <p>Contact your TSM with any public IP addresses or ranges that you would like to add to this list.</p> <p>Admin users can add, edit or delete subnets in an account.. See <a href="#">Add or edit a subnet on page 156</a></p> |
| <b>Device Tracking</b> | <p>Use this page to exclude or delete a device from your account.</p> <p>Devices in this list will not have any new DHCP device tracking collected. The device tracking information is visible in the DHCP section of the <a href="#">Entity Panel</a> and the <a href="#">Sensor Device View</a> section when viewing by visible devices.</p> <p>To exclude devices from detections, see <a href="#">Excluding Devices</a> under <i>Detections</i>.</p>   |
| <b>Modules</b>         | Displays the available integrations for FortiNDR Cloud.  |

|                 |  |
|-----------------|--|
| <b>Settings</b> | Enable SAML SSO, multi-factor authentication, and generate PCAP encryption keys.   |
| <b>Billing</b>  | <p>Displays the billing summary of the daily and monthly bandwidth usage for an account. Accounts are billed based on the 95th percentile of the aggregate bandwidth usage across all sensors over 10-second intervals. The daily and Month-To-Date (MTD) numbers are calculated after the end of each UTC day.</p> <ul style="list-style-type: none"> <li>The <i>Billing</i> tab displays the: <ul style="list-style-type: none"> <li><i>Billing Summary</i>: Your account's bandwidth usage, for the current date, as compared to your available license.</li> <li><i>Monthly History</i>: The historical data of the bandwidth usage for the chosen date range. You can also compare the bandwidth usage between two or more months by selecting the appropriate date range.</li> </ul> </li> <li>The <i>Daily Stats</i> tab displays the daily bandwidth usage for the chosen date range.</li> </ul> <p>For customers with more than one account, the billing summary will display the bandwidth for both the parent and child accounts. Click the arrow next to the account name to toggle between the parent and child views. Use the date picker to view the bandwidth for a previous month in the billing cycle.</p> |

## Creating users and assigning roles

Go to *Account Management > Users* to add users and assign roles. You also have the option of creating API Only users. The User Management table displays all the users with access to the portal. A green Admin icon appears next to the email addresses of users with Admin privileges.

The *Account Management > Users* page displays the following information:

| Column            | Description   |
|-------------------|---|
| <b>Email</b>      | The user's email address                                      |
| <b>Full Name</b>  | The user's full name.   |
| <b>First Name</b> | The user's first name.  |
| <b>Last Name</b>  | The user's last name.   |
| <b>UUID</b>       | The user's unique ID.   |
| <b>Last Login</b> | The date and time the user last logged into the account.      |
| <b>Created</b>    | The date the user was created.                                |
| <b>Updated</b>    | The date and time the user's details were updated.            |
| <b>Status</b>     | The user's current status ( <i>Enabled/Disabled</i> ).        |
| <b>Locked Out</b> | Indicates the user has been locked out of the account.        |
| <b>MFA</b>        | Indicates Multi-Factor Authentication is enabled or disabled. |
| <b>Roles</b>      | The user role. This column is not displayed by default.       |

| Column         | Description   |
|----------------|---|
| <b>Actions</b> | Use the menu in this column to: <ul style="list-style-type: none"> <li>• Edit the user details</li> <li>• Move the user between accounts</li> <li>• Email/reset the password.</li> <li>• Disable the user.</li> </ul> |

### To create a new user:

1. Click the gear icon at the top-right of the page and select *Account Management*. (Click the *Users* tab if it is not already open.)



2. Click *Create User*. The *Create New User* dialog opens.
3. Enter the user's details. Required fields are indicated with an asterisk (\*).

|                    |   |
|--------------------|---|
| <b>Email</b>       | Enter the user's email address.   |
| <b>First name</b>  | Enter the user's first name.  |
| <b>Last name</b>   | Enter the user's last name.   |
| <b>Assign role</b> | Select one of the following options. <ul style="list-style-type: none"> <li>• <i>User</i></li> <li>• <i>Limited User</i></li> <li>• <i>Admin</i></li> </ul>   |
| <b>API Only</b>    | <p><i>API-only users</i> are primarily designed for integration configurations. They cannot have passwords or multi-factor authentication enabled, they do not receive emails, and their keys are managed entirely by those with <i>Admin</i> privileges for the account.</p> <p>API-only users do not appear in the user list by default, but can be displayed by adjusting the page filters. See, <a href="#">To filter the user list</a>.</p> <hr/> <div style="display: flex; align-items: center;"> <p><i>API Only</i> is the user role when mandatory SSO is enabled. See <a href="#">Settings (Account Management)</a> on page 151.</p> </div> |

4. Click *Create*.



New users are automatically assigned the *Training User* role on the Training Modern account, even if the administrator has not assigned any roles to the user. If the account is a parent account, and the administrator has access to child accounts, then a checkbox is available to include child accounts.

**To view user details:**

- Double-click a user in the list. The user details pane opens.

**test user** ✕

EMAIL: testuser@gmail.com

CREATED: 2023-10-25 02:52:24 (UTC)

UPDATED: 2023-10-25 02:52:24 (UTC)

MFA: DISABLED

TYPE: Portal User

STATUS: ENABLED

Edit Move Assign Role Reset Password Disable User

**ROLES**

| Role          | Account    | Actions |
|---------------|------------|---------|
| Admin         | [REDACTED] | -       |
| Admin         | [REDACTED] | -       |
| User          | [REDACTED] | -       |
| User          | [REDACTED] | -       |
| Admin         | [REDACTED] | -       |
| Training User | [REDACTED] | -       |
| Admin         | [REDACTED] | -       |



- The following icon indicates the user belongs to child accounts.
- *Edit* and *Reset Password* are disabled with mandatory SSO is enabled. See [Settings \(Account Management\)](#) on page 151.

**To filter the user list:**

1. Click the Filter icon.



2. Select the filter type.

|                       |   |
|-----------------------|---|
| <b>Status</b>         | Select <i>All</i> , <i>Enabled</i> or <i>Disabled</i> . |
| <b>User Type</b>      | Select <i>All</i> , <i>Portal</i> or <i>API Only</i> .  |
| <b>Account Access</b> | Select an account from the dropdown list.               |
| <b>User Role</b>      | Select a user role from the dropdown list.              |

**To update a user's details:**

1. Click a user in the list. The *User Details* pane opens.

| Option                | Purpose   |
|-----------------------|---|
| <b>Edit</b>           | Modify the email or name for the user account.  |
| <b>Move</b>           | Assign the user to a different account.   |
| <b>Assign Role</b>    | Assign a role to a user. <ul style="list-style-type: none"> <li>• <i>User</i></li> <li>• <i>Limited User</i></li> <li>• <i>Admin</i></li> </ul>                                 |
| <b>Reset Password</b> | Send an email with a password reset link to the user.   |
| <b>Disable MFA</b>    | Disable the requirement for an MFA token for the user. If <i>Require MFA</i> is enabled for the account, the user will be required to re-establish an MFA token on next log in. |
| <b>Unlock</b>         | Unlock the user account. User accounts are locked after five failed password attempts in 10 minutes.  |
| <b>Disable User</b>   | Disable log in access to the user account and any of its API tokens.  |



Optionally, you can use the menu in the *Actions* column to quickly *Edit User*, *Move User*, *Email Password Reset* or *Disable User*.

The *Edit User* and *Email Password Reset* are disabled when mandatory SSO is enabled. See [Settings \(Account Management\) on page 151](#).

2. Click close (X) to close the pane.

**To perform bulk actions:**

1. Select the users in the lists or select all. The tools icon is activated.



2. Click the tool icon and select *Move Users*, *Enable Users*, *Disable Users*, *Assign Role* or *Revoke Role*.

**To export the user list as a CSV file:**

- In the toolbar, click the CSV button. The list is saved to your device.



In the *user\_role* column, if the user has:

- No account name in front of the role, this indicates the user belongs to the current account (Admin, User, Limited User).
- The same role in two or more accounts, the account name is displayed followed by a colon (:) followed by the user role.

## Settings (Account Management)

Use the settings tab to upload and upgrade PCAP encryption keys, enable and update SAML SSO settings, and enable multi-factor authentication.

- [SAML SSO](#)
- [PCAP encryption keys](#)
- [Multi-factor authentication](#)
- [Disable an Account](#)
- [Sensor email alerts](#)

### SAML SSO

FortiNDR Cloud translates SAML authentication from the identity provider into the native authentication scheme. User login is the same regardless of whether the user has logged in using SAML or a password. The session state in FortiNDR Cloud is independent of the SAML session. Logging out of SAML does not log the user out of FortiNDR Cloud.

When enabling SAML SSO keep the following considerations in mind:

- First time FortiNDR Cloud users will have a user record created automatically when they first authenticate using SAML. Users are required to have a first name, but the last name is optional. These users will initially have no permissions. An Admin will need to grant roles to these users using the normal Account Management UI.
- When existing users authenticate using SAML, any changes to their first and last name will be updated in FortiNDR Cloud as well.
- FortiNDR Cloud identifies users from SAML by their email address. If the user's email address has changed in the SAML SSO Provider, FortiNDR Cloud will create a new user record for that user the next time they log in.
- Disabling a user in FortiNDR Cloud also disables SAML authentication for that user. However, disabling a user in the SAML SSO Provider does not disable the user in FortiNDR Cloud. The user will still have access if they have a password or permanent token. Users need to be manually disabled in FortiNDR Cloud as well.
- Users authenticating with SAML are also allowed to authenticate using passwords as well. Typically, at least one Admin in the account should have a password as a backup in case SAML authentication fails.

### Failure Scenarios

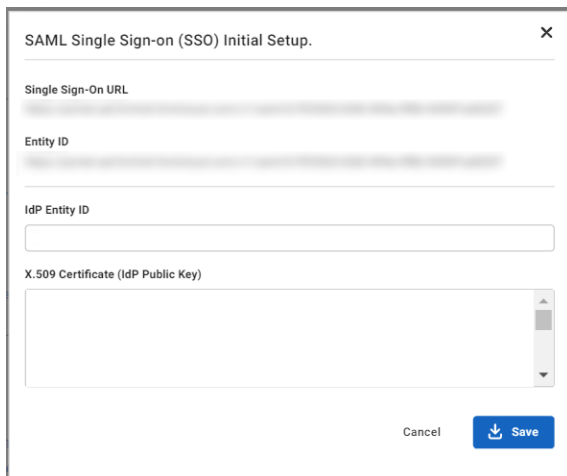
There are a variety of reasons why SAML authentication may fail.

- SAML has not been configured for the account.
- SAML has been configured, but disabled.
- The user is attempting to authenticate with the wrong account. For example, the user belongs to the Acme account but is trying to authenticate with the Acme Subsidiary account.
- The user has been disabled in FortiNDR Cloud.
- The user does not have a first name.

For security reasons, FortiNDR Cloud may not provide the exact reason for the failure. Please make sure that SAML is configured correctly for the account and the user.

**To enable SAML login:**

1. Click the gear icon in the top navigation and select *Account Management*.
  - If you have access to one account, the account page will appear.
  - If you have access to multiple accounts, select an account.
2. Click the *Settings* tab.
3. Click *Set up SAML SSO*. The "*SAML Single Sign-on (SSO) Initial Setup*" dialog opens.



4. Copy the values from the *Single Sign-On URL* and *Entity ID* fields and paste them into the general settings of your SAML Provider configuration.



*Entity ID*" may also be called "*Audience URI*" or "*SP Entity ID*".

5. Set the application's subject or username to *Email*. For example, in the Okta setup, select *Email* from the *Application username* field.
6. Add an attribute statement, *first\_name*, with the value for a user's first name. For example in Okta's Attribute Statements settings, enter *first\_name* in the *Name* field and then select *user.firstName* from the *Value* field.
7. Add an attribute statement, *last\_name*, with the value for a user's last name.
8. Supply the following information from your SAML SSO Provider into the *SAML Single Sign-on (SSO) Initial Setup* dialog:
  - *IdP Entity ID*
  - *X.509 Certificate (IdP Public Key)*
9. Click **Save**.

**To login with SAML SSO:**

1. Navigate to your SAML SSO Provider's dashboard
2. Click the ThreatINSIGHT or FortiNDR Cloud button from the SAML SSO Provider's dashboard





- FortiNDR Cloud only supports IdP (identity-provider) initiated logins where the user will need to initiate login from their SAML SSP Provider's dashboard.
  - If you are a new user logging into FortiNDR Cloud for the first time, you will see a message indicating that you do not have permission to use this application. This means that your roles have not yet been granted. Contact your administrator to assign your roles.
- 

1. Click the gear icon in the top navigation and select *Account Management*.
  - If you have access to one account, the account page will appear.
  - If you have access to multiple accounts, select an account.
2. Click the *Settings* tab and click *Disable SAML Settings*.
3. In the Confirmation Dialog, click *Confirm*.

## Mandatory SSO

You can require all users to log into FortiNDR Cloud using SSO. Before enabling mandatory SSO, keep the following considerations in mind:

- Multi-Factor Authentication (MFA) is disabled.
- You can only edit API users
- *Change my password* and *Enable MFA* are disabled in *Profile Settings > My Profile > Authentication*
- *Edit User* and *Email Password Reset* are disabled in *Account Management > Users > Actions*.

### Requirements:

- SAML SSO must be enabled.
- User must have *account.sso\_required.update* permissions

### To enable mandatory SSO:

1. Click the gear icon in the top navigation and select *Account Management*.
  - If you have access to one account, the account page will appear.
  - If you have access to multiple accounts, select an account.
2. Click the *Settings* tab.
3. Under *SAML SSO* enable *Require SSO Login (disable login with username/password)*. The *Confirm enabling mandatory SSO login* dialog opens.
4. Click *Confirm*

## PCAP encryption keys

PCAP Encryption Keys are used in conjunction with Packet Capture. If an encryption key is uploading, all PCAP files will be encrypted with the provided key. This prevents FortiNDR Cloud from having any visibility into the raw PCAP data that was captured. For more information, see [Packet Capture on page 107](#).

---



The corresponding private key will be required to decrypt any downloaded PCAP files. If the private key is lost, the encrypted PCAP files cannot be recovered.

---

### To upload an encryption key:

1. Click the gear icon in the top navigation and select *Account Management*.
  - If you have access to one account, the account page will appear.
  - If you have access to multiple accounts, select an account.
2. Click the *Settings* tab.
3. Under *PCAP ENCRYPTION KEYS*, click *Set PCAP Encryption Key*. The *Set PCAP Encryption Key* dialog opens.
4. Paste the public key and click *Set Key*.

The key will take effect for any new PCAP files generated. Existing PCAP files are not retroactively encrypted.

## Multi-factor authentication

Enable Multi-factor authentication (MFA) require all users to enter an MFA token the next time they log in to FortiNDR Cloud. Users will not be able to navigate to any FortiNDR Cloud page until they confirm their MFA token.

### To enable Multi-factor authentication:

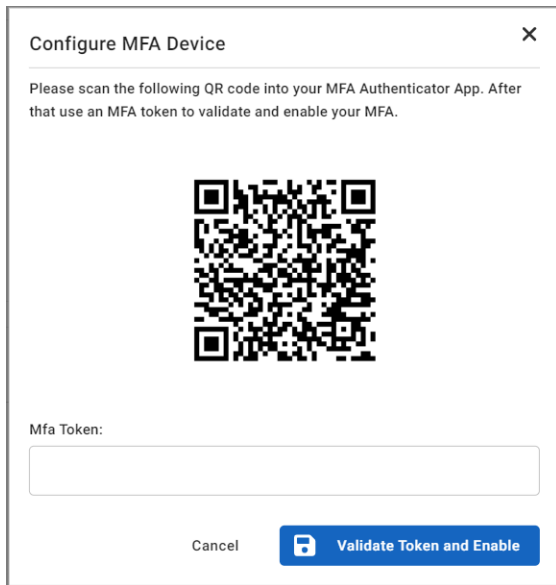
1. Click the gear icon at the top-right of the page and select *Profile Settings*.

The screenshot shows the FortiNDR Cloud dashboard. The top navigation bar includes 'Dashboard', 'Detections', 'Investigations', and 'Reports'. A search bar and 'Entity' dropdown are also present. The time is 14:50:09 UTC. On the right side, a gear icon is highlighted with a red box, and a dropdown menu is open, showing 'Profile Settings' as the selected option. Below the navigation bar, the dashboard displays 'MITRE ATT&K Detections Activity' with a bar chart showing detection counts for various categories like Reconnaissance, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. The 'Observations' section on the right shows a table with columns for 'Observation Title', '02/28 - 03/05', and '03/06'. The table lists 'Anomalous Active Directory Enum...', 'New Internal Enumeration Source', and 'Malicious PE File' with their respective counts. A line chart below the table shows the trend of these observations over time.

2. Under *Authentication*, click *Enable MFA*.


The screenshot shows the 'Authentication' settings page. The page title is 'Authentication' and the subtitle is 'User authentication settings'. There are two main sections: 'Password' and 'Multi-Factor Authentication'. The 'Password' section has a 'Change my password' button. The 'Multi-Factor Authentication' section has an 'Enable MFA' button. Below these sections, there is a note: 'You need FortiToken, Google Authenticator or another app that supports TOTP.' Below this note, there are links for 'iPhone: FortiToken Google Authenticator' and 'Android: FortiToken Google Authenticator'.

3. Scan the QR code with a token application to validate and enable MFA.



Configure MFA Device

Please scan the following QR code into your MFA Authenticator App. After that use an MFA token to validate and enable your MFA.



Mfa Token:

Cancel Validate Token and Enable

## Disable an Account

Technical Success Managers can disable accounts that are either no longer in use or should no longer be in use. This option has the following effects:

- Disables login for all users in the account.
- Disables all notifications to those users.
- Stops ingest of all data.
- Removes the account from default account lists.

This can be completed by clicking the option icon in Account Management for a given account and then clicking on *Disable*.

## Sensor email alerts

Administrators can create email notifications to alert you when sensor is offline or the event rate is low.

### To create a sensor email alert:

1. Click the gear icon in the top navigation and select *Account Management*.
  - If you have access to one account, the account page will appear.
  - If you have access to multiple accounts, select an account.
2. Click the *Settings* tab and scroll down to *Notification Emails*.
3. In the *Email* field, enter a recipient's email address.
4. Select *Sensor Offline Alert* and/or *Event Rate Low Alert*.
5. Click *Update*.
6. Click *Add Record* to add another email address.
7. Click **X** to delete an email address.

## Add or edit a subnet

The *Subnets* page lists all internal IP address ranges for the account. Admin users can add, edit or delete subnets in an account.

### To add a subnet:

1. Click the gear icon in the top navigation and select *Account Management*.
  - If you have access to one account, the account page will appear.
  - If you have access to multiple accounts, select an account.
2. Click the *Subnets* tab and click *Add Subnet*. The *Add a Subnet* dialog opens.
3. Configure the subnet and click *Add Subnet*.

|                    |  |
|--------------------|--|
| <b>Subnet</b>      | Enter the IP address for the subnet.   |
| <b>Description</b> | (Optional) Enter a description of the subnet.                                      |
| <b>External</b>    | Select if this is an internal subnet that will be treated as external by Suricata. |

Add a Subnet

Subnet \*

###.###.###.###

Description

An optional description of this subnet.

External

Cancel

Add Subnet

### To edit a subnet:

1. Click the gear icon in the top navigation and select *Account Management*.
2. Click the *Subnets* tab.
3. In the *Actions* column, click the dropdown and select *Edit*. The *Update Subnet* dialog opens.
4. Edit the subnet and click *Update Subnet*.

### To delete a subnet:

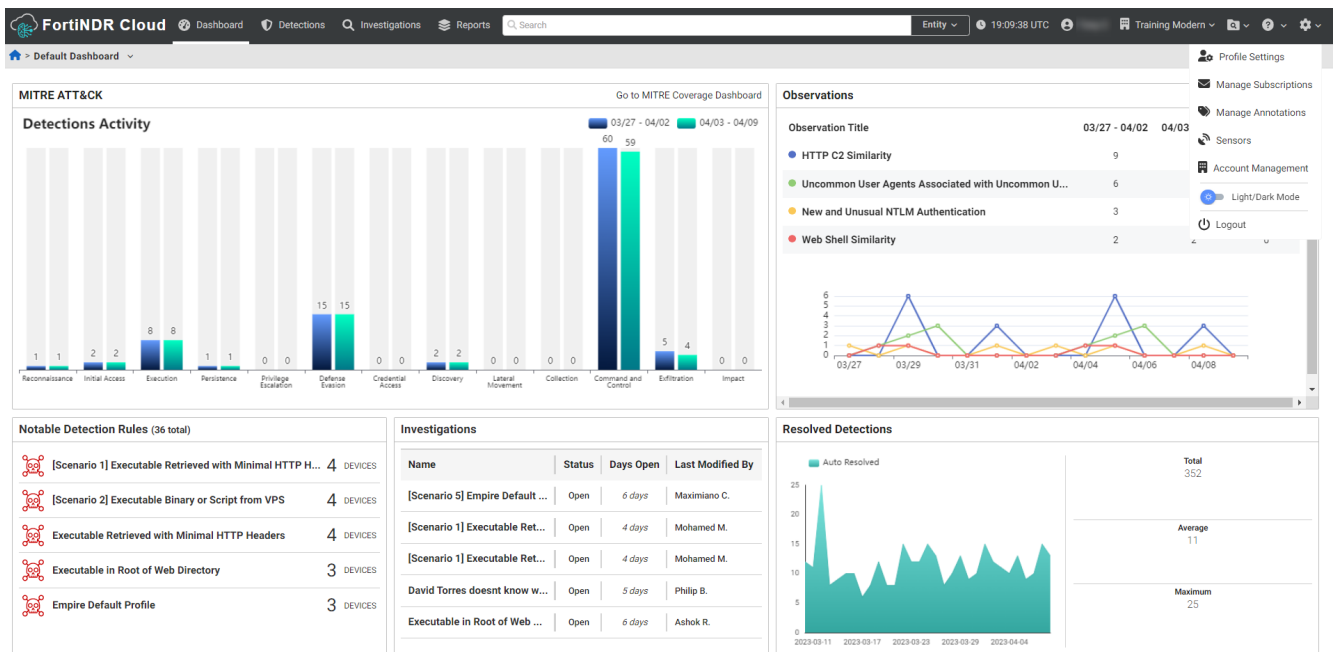
1. Click the gear icon in the top navigation and select *Account Management*.
2. Click the *Subnets* tab.
3. In the *Actions* column, click the dropdown and select *Delete*. The *Delete xx.xx.xxx.x/xx?* dialog opens.
4. Click *Confirm*.

## Light/Dark Mode

The Light/Dark mode setting is saved to your browser. When you switch accounts, you will see the same theme as the previous user account. The mode you select does not affect other users with the same account.

### To switch between light and dark mode:

Click the gear icon at the top-right of the page and toggle between *Light* and *Dark* mode.



# Sensors deployment

FortiNDR Cloud deploys network sensors to monitor your virtual and physical on-premises infrastructure. Once deployed and configured, network metadata is collected and sent to FortiNDR Cloud for security analysis, threat detection, and indexing. A web application and application programming interface (API) are provided for analysis of security events. FortiNDR Cloud is delivered as a Software-as-a-Service (SaaS) and is fully managed by Fortinet, including network sensors.

The maximum size of the folder that stores the logs is 10G. Sensors are designed to retain logs for seven days. In the event of an issue affecting the upload, logs that are seven days and older will expire and are no longer available. Cleanup scripts are in place to automatically clean up the files when the log directory exceeds a certain size to prevent excessive disk usage.

## Sensor specifications

### Sensor Types

The following table lists the available sensor types and the maximum sustained throughput each type can consume.

| Sensor Type | Form      | Max Sustained Bandwidth |
|-------------|-----------|-------------------------|
| Small       | 1U Server | 2Gbps                   |
| Large       | 1U Server | 10Gbps                  |
| Virtual     | OVF File  | 1.5Gbps                 |

### Network interfaces for physical sensors

- 1 x 1Gbps Ethernet interface for management
- 1 x 1Gbps Ethernet interface for monitoring
- 2 x 10Gbps Ethernet interfaces for monitoring
- 2 x 10Gbps SFP (fiber) interfaces for monitoring

### Minimum virtual sensor (ESX) host requirement

For details, the [ESXi Sensor Installation Guide](#).

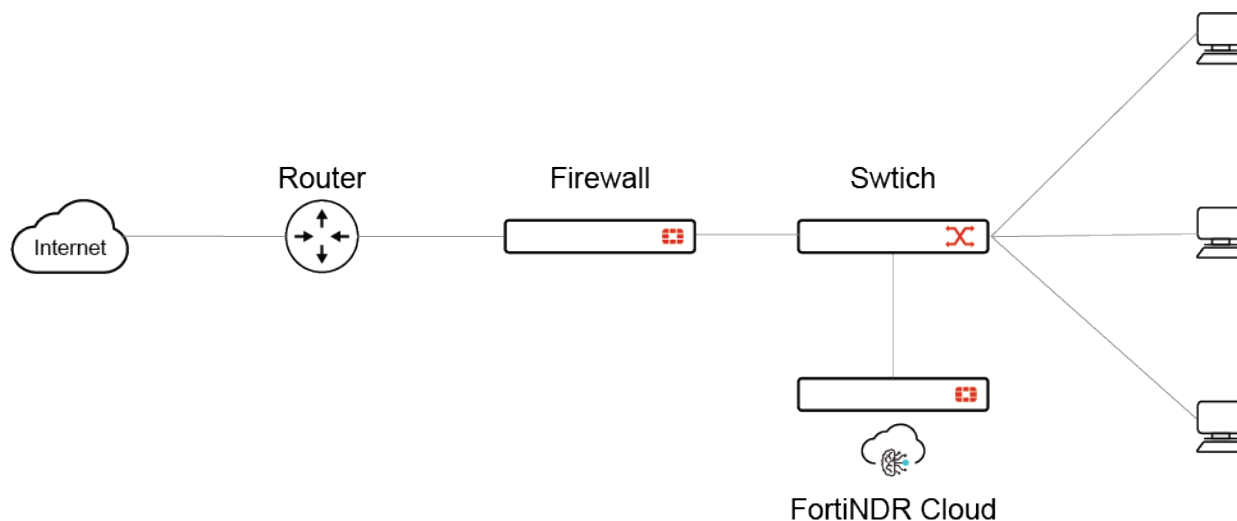
## Network data sources

A network data source must be configured for the sensor. Sensors collect and process network data using standard network packet capture sources such as a network switch Switched Port Analyzer (SPAN) port or Test Access Port (TAP) device connected to a monitoring interface on the sensor. Virtual sensors do not currently support ERSPAN data sources.

### SPAN (mirror) port

A SPAN port (sometimes called a mirror port) is a software feature built into a switch that creates a copy of selected packets passing through the device and sends them to a designated SPAN port. Using software on the network switch, an administrator can easily configure what data is monitored by a FortiNDR Cloud sensor connected to the SPAN port.

If the switch CPU is already heavily utilized prior to configuring a SPAN, SPAN data will likely be given a lower priority on the switch. The SPAN also uses a single egress port to aggregate multiple links, so it may become oversubscribed.



### When to consider a SPAN port

- Limited ad hoc monitoring in locations with SPAN capabilities where a network TAP does not currently exist.
- Production emergencies where there is no maintenance window in which to install a TAP.
- Remote locations with modest traffic that cannot justify a full-time TAP on the link.
- Access to traffic that either stays within a switch or never reaches a physical link where the traffic can be TAPed.
- Locations with limited light budgets where the split ratio of a TAP may consume too much light.

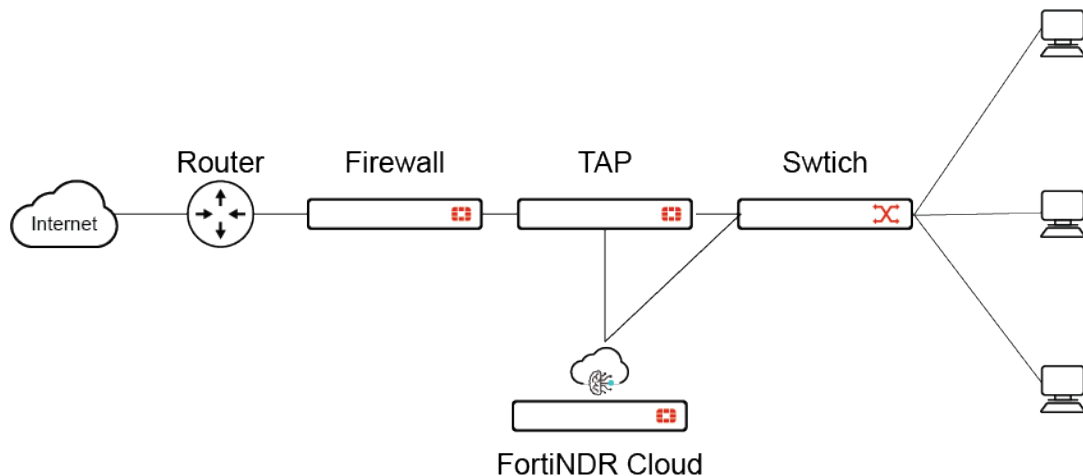
## Network TAP

A network TAP (Test Access Point) is a device that connects directly to the cabling infrastructure. Instead of two switches or routers connecting directly to each other, the network TAP sits between the two devices and all data flows through the TAP. Using an internal splitter, the TAP creates a copy of the data for monitoring while the original data continues unimpeded through the network.

This ensures every packet of any size will be copied. This technique also eliminates any chance of subscription overage. Once the data is TAPed, the duplicate copy can be sent to a FortiNDR Cloud sensor.



Inserting a TAP into an existing network link requires a brief cable disconnect. TAPs are typically installed during a maintenance window.



### When to consider a network TAP

- Switch CPU already highly utilized and may drop packets.
- When additional load on the switch could impact network performance.
- No ports available on the switch.
- Hardware does not support SPAN functionality.
- When legal regulations or corporate compliance mandate that all traffic for a particular segment be monitored.

Not sure which data source(s) to use? Ask your FortiNDR Cloud representative.

### Network aggregator

For many organizations, a network aggregator is configured to monitor traffic at several key locations within the network. FortiNDR Cloud sensors can deploy off a network aggregator if one is available within the network. Some network aggregation appliances also have the ability to decrypt network traffic, which can greatly increase the fidelity and visibility of the FortiNDR Cloud sensor.

Network aggregators are also commonly used to monitor traffic from networks with 40Gbps links. In this case, an aggregator is utilized to split traffic from a 40Gbps line to four separate FortiNDR Cloud appliances monitoring up to 10Gbps per sensor.

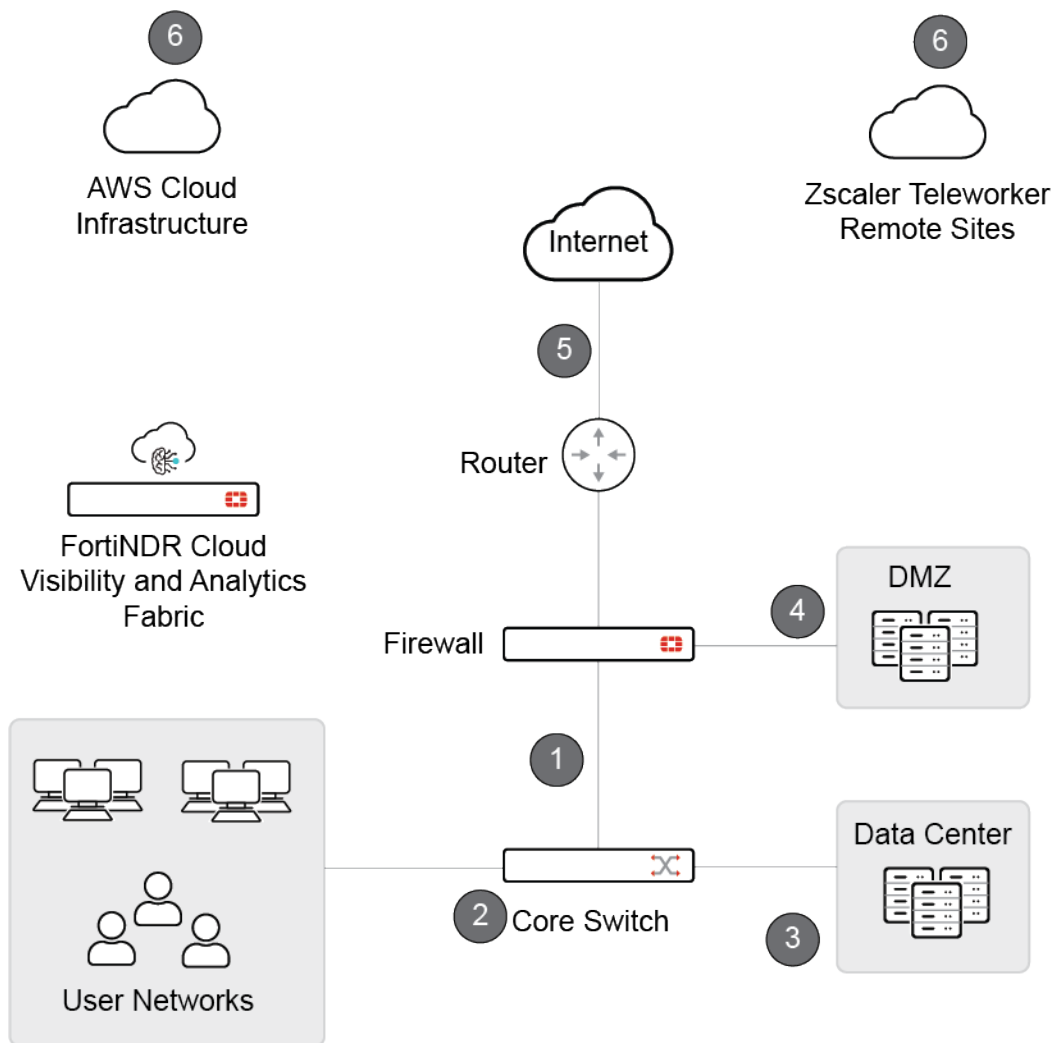


## Complex or combination deployments

Multiple FortiNDR Cloud sensors can be deployed to obtain full visibility across the environment. Each sensor reports back to the FortiNDR Cloud, providing cross-enterprise visibility through a single, unified platform. Queries can be executed against data from all sensors, or a subset as specified by an analyst.

## Sensor deployment strategy

Sensor placement is prioritized for network locations where security events are most likely to occur. Data collected from multiple locations provides a complete and accurate picture of potential security threats. Below is a prioritized list of data source locations in a typical network environment.



| Number | Location             | Description   |
|--------|----------------------|---|
| 1      | <b>Egress Points</b> | <p>Monitoring activity between your network environment and the Internet provides visibility of security events related to malware beaconing, command and control, network tunneling and data exfiltration activity.</p> <p>Benefits:</p> <ul style="list-style-type: none"> <li>• Captures north/south traffic from clients and servers</li> <li>• Enables detection of exfiltration, C2, tunneling, beaconing</li> </ul>  |
| 2      | <b>Core Switch</b>   | <p>Activity within your network can include security events related to lateral movement and staging of attacks between workstations and important internal resources such as internal web applications, file servers or your system infrastructure.</p> <p>Benefits:</p> <ul style="list-style-type: none"> <li>• Captures east/west traffic between clients and servers</li> <li>• Enables detection of lateral movement, staging, internal threats</li> </ul>   |
| 3      | <b>Data Center</b>   | <p>Your data center infrastructure is where your valuable information is stored, making it a target for theft and unauthorized access. Sensors placed between these servers and virtual hosts provide visibility of security events related to this activity.</p> <p>Benefits:</p> <ul style="list-style-type: none"> <li>• Captures east/west traffic between servers (including virtual)</li> <li>• Enables detection of data theft, unauthorized access</li> </ul>   |
| 4      | <b>DMZ</b>           | <p>Public facing applications such as mail services, web sites and business-to-business applications are constantly attacked. Monitoring network zones that host these applications provides visibility of security events related to unauthorized access and data exfiltration.</p> <p>Benefits:</p> <ul style="list-style-type: none"> <li>• Captures north/south traffic between DMZ and external clients</li> <li>• Enables detection of unauthorized access, vulnerability exploitation, exfiltration</li> </ul> |
| 5      | <b>External Link</b> | <p>Benefits:</p> <ul style="list-style-type: none"> <li>• Captures north/south traffic between external clients and the internal networks. Provides visibility to traffic even if it is blocked by the firewall</li> <li>• Enables detection of exploitation attempts</li> </ul>  |

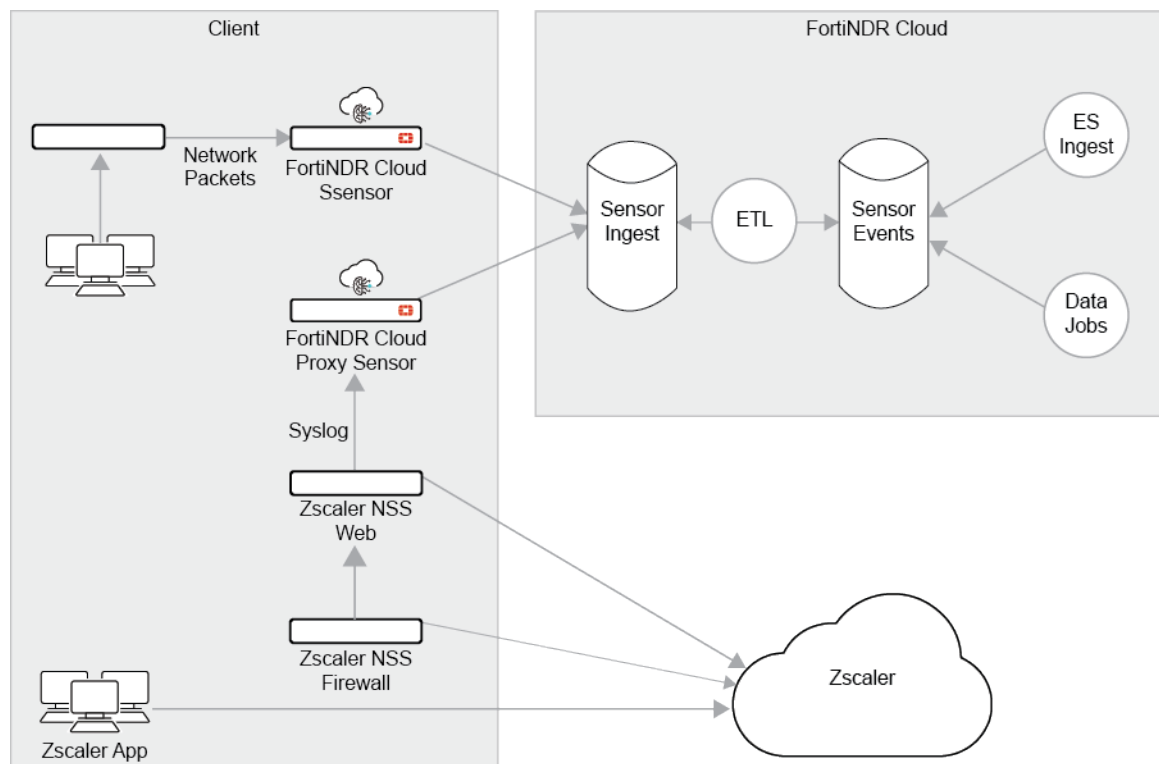
| Number | Location         | Description   |
|--------|------------------|---|
| 6      | Cloud Visibility | <p>Benefits:</p> <ul style="list-style-type: none"> <li>• Cloud infrastructure workload traffic analysis via AWS/Azure Machine Images or VM/KVM.</li> <li>• Teleworker and Remote Sites not backhauled to VPN via Zscaler integration.</li> <li>• Enables detection of un-managed and IoT devices and access to cloud infrastructure</li> </ul> |

## Sensor data source configuration

For instructions on sensor data source configuration for VMware ESX, see the [ESXi Sensor Installation Guide](#).

## Zscaler ingestion

You can upload your network metadata from Zscaler the same way that you can upload data from FortiNDR Cloud sensors running Zeek.



## Available features

Not all existing FortiNDR Cloud features are supported with Zscaler.

| Feature                | Available | Comments   |
|------------------------|-----------|--|
| <b>Event Search</b>    | Yes       | On a subset of event types and fields.   |
| <b>Detections</b>      | Partial   | Existing detection rules will initially be excluded from Zscaler. ATR will selectively enable rules that they believe are compatible. Customers will not be able to create rules that match Zscaler events. Detections will not match for customers using the Zscaler Connector App. See the Network Locality section below. |
| <b>First/last seen</b> |           | Requires porting the data job from the legacy ETL.   |
| <b>Passive DNS</b>     | Yes       | Requires porting the data job from the legacy ETL.   |
| <b>Devices</b>         |           | Requires porting the data job from the legacy ETL.   |

## Deployment services

You will need to deploy three separate services on your system:

1. A Zscaler NSS instance for web logs. This is required for HTTP and SSL events.
2. A Zscaler NSS instance for firewall logs. This is required for DNS and Flow events.
3. A Fortinet proxy sensor to receive the logs from NSS and upload them to FortiNDR Cloud.

## Zscaler setup

### Zscaler NSS

NSS stands for [Nanolog Streaming Service](#). It is a Zscaler provided utility to download logs. Note that Zscaler requires separate instances for web and firewall logs. Customers that already ingest Zscaler data may have NSS instances that can be used for FortiNDR Cloud. If you do not have NSS installed, you should contact Zscaler for help.

### Proxy sensor

NSS forwards logs using the syslog protocol. The proxy sensor is designed to receive these logs and upload them to the same destination as FortiNDR Cloud sensors. Once ingested, the Zscaler events are mostly treated the same as Zeek events.



The Docker Container must be run from a system that is separate from the NSS log server.

## NSS feed configuration

Once the NSS and proxy sensor instances have been deployed, feeds have to be configured to enable logging. Please refer to the Zscaler's [About NSS Feeds](#) page if you need help.

### Configuration Issues

It is important that the feeds are configured correctly. If the system is not configured correctly there will be data loss. In the worst case scenario, it may cause problems with the ingest pipeline.

### Base Configuration



All feeds share the same base configuration:

#### Web

- **Feed Name**  
FortiNDR Cloud - Web
- **NSS Type**  
NSS for Web
- **Log Type**  
Web Log
- **Feed Output Format**

```
zscaler_log_type=web\timestamp=%d{yyyy}-%02d{mth}-%02d{dd}T%02d{hh}:%02d{mm}:%02d
{ss}Z\tzscaler_recordid=%d{recordid}\tzscaler_proto=%s{proto}\tsrc_ip=%s{cip}\tdst_ip=%s
{sip}\tstatus_code=%s{respcode}\tmethod=%s{reqmethod}\tuser_agent=%s{ua}\treferrer=%s
{ereferer}\trequest_length=%d{reqsize}\tresponse_length=%d{respsize}\turi=%s
{eurl}\tfile_md5=%s{bamd5}\tcontent_type=%s{contenttype}\tclient_cipher=%s
{clientsslcipher}\tclient_version=%s{clienttlsversion}\tserver_cipher=%s
{srvsslcipher}\tserver_version=%s{srvtlsversion}\tzscaler_username=%s{login}\tzscaler_
hostname=%s{devicehostname}
```

Example:

Add NSS Feed
✕

**NSS FEED**

**Feed Name**  
FortiNDR Cloud - Web

**NSS Server**  
NONE

**SIEM Destination Type**  
 IP Address  FQDN

**SIEM TCP Port**  
\_\_\_\_\_

**SIEM Rate**  
 Unlimited  Limited

**Log Type**  
 Web Log  Tunnel  Alert

**Feed Output Type**  
Custom

**Feed Output Format**  

```
zscaler_log_type=web&ttimestamp=%d{yyyy}-%02d{mth}-%02d{dd}T%02d{hh}:%02d{mm}:%02d{ss}Z\tzscaler_recordid=%d{recordid}\tzscaler_proto=%s{proto}\tsrc_ip=%s{cip}\tdst_ip=%s{sip}\tstatus_code=%s{respcode}\tmethod=%s{reqmethod}\tuser_agent=%s{ua}\treferer=%s{ereferer}\trequest_length=%d{reqsize}\tresponse_length=%d{respsize}\turi=%s{eurl}\tfile_md5=%s{bamd5}\tcontent_type=%s{contenttype}\tclient_cipher=%s{clientsslcipher}\tclient_version=%s{clienttlsversion}\tserver_cipher=%s{srvsslcipher}\tserver_version=%s{srvtlsversion}
```

**User Obfuscation**  
 Enabled  Disabled

**Duplicate Logs**  
Disabled

**NSS Type**  
 NSS for Web  NSS for Firewall

**Status**  
 Enabled  Disabled

**SIEM IP Address**  
\_\_\_\_\_

**Feed Escape Character**  
\_\_\_\_\_

**Timezone**  
GMT

| ACTION                      | WHO | FROM WHERE | TRANSACTION | TO WHERE                    | SECURITY | FILE TYPE | DLP |
|-----------------------------|-----|------------|-------------|-----------------------------|----------|-----------|-----|
| <b>WEB LOG FILTERS</b>      |     |            |             |                             |          |           |     |
| <b>Policy Action</b><br>ANY |     |            |             | <b>Policy Reason</b><br>Any |          |           |     |

Save
Cancel

## DNS

- **Feed Name**  
FortiNDR Cloud - DNS
- **NSS Type**  
NSS for Firewall
- **Log Type**  
DNS Logs
- **Feed Output Format**

```
zscaler_log_type=dns\ttimestamp=%d{yyyy}-%02d{mth}-%02d{dd}T%02d{hh}:%02d{mm}:%02d{ss}Z\tzscaler_recordid=%d{recordid}\tsrc_ip=%s{cip}\tdst_ip=%s{sip}\tdst_port=%d{sport}\tquery=%s{req}\tqtype_name=%s{reqtype}\tresponse=%s{res}\tzscaler_username=%s{login}\tzscaler_hostname=%s{devicehostname}
```

### Example

Add NSS Feed
✕

**NSS FEED**

**Feed Name**  
FortiNDR Cloud - DNS

---

**NSS Server**  
NONE

---

**SIEM Destination Type**  
 IP Address     FQDN

**SIEM TCP Port**  


---

**SIEM Rate**  
 Unlimited     Limited

**Log Type**  
 Firewall Logs     DNS Logs     Alert

**Feed Output Type**  
Custom

---

**Feed Output Format**  

```
zscaler_log_type=dns&timestamp=%d{yyyy}-%02d{mth}-%02d{dd}T%02d{hh}:%02d{mm}:%02d{ss}Z\tzscaler_recordid=%d{recordid}\tsrc_ip=%s{cip}\tdst_ip=%s{sip}\tdst_port=%d{sport}\tquery=%s{req}\tqtype_name=%s{reqtype}\tresponse=%s{res}
```

**NSS Type**  
 NSS for Web     NSS for Firewall

**Status**  
 Enabled     Disabled

**SIEM IP Address**  


---

**Feed Escape Character**  


---

**User Obfuscation**  
 Enabled     Disabled

**Timezone**  
GMT

---

**Duplicate Logs**  
Disabled

| ACTION                       | WHO | SOURCE | DESTINATION              | SESSION |
|------------------------------|-----|--------|--------------------------|---------|
| <b>DNS FILTERS</b>           |     |        |                          |         |
| <b>Policy Actions</b><br>Any |     |        | <b>Rule Names</b><br>Any |         |

Save
Cancel



## Firewall

- **Feed Name**

FortiNDR Cloud - Firewall

- **NSS Type**

NSS for Firewall

- **Log Type**

Firewall Logs

- **Feed Output Format**

```
zscaler_log_type=firewall\timestamp=%d{yyyy}-%02d{mth}-%02d{dd}T%02d{hh}:%02d{mm}:%02d{ss}Z\tzscaler_recordid=%d{recordid}\tsrc_ip=%s{csip}\tsrc_port=%d{cspport}\tdst_ip=%s{cdip}\tdst_port=%d{cdport}\tduration=%d{durationms}\tprotocol=%s{ipproto}\tservice=%s{nwsvc}\trequest_bytes=%ld{outbytes}\tresponse_bytes=%ld{inbytes}\tzscaler_username=%s{login}\tzscaler_hostname=%s{devicehostname}
```

### Example

Add NSS Feed
✕

**NSS FEED**

**Feed Name**  
FortiNDR Cloud - Firewall

---

**NSS Server**  
NONE

---

**SIEM Destination Type**  
 IP Address  FQDN

---

**SIEM TCP Port**  
\_\_\_\_\_

---

**SIEM Rate**  
 Unlimited  Limited

---

**Log Type**  
 Firewall Logs  DNS Logs  Alert

---

**Firewall Log Type**  
 Full Session Logs  Aggregate Logs  Both Session and Aggregate Logs

---

**Feed Output Type**  
Custom

---

**Feed Output Format**  

```
zscaler_log_type=firewall\ttimestamp=%d{yyyy}-%02d{mth}-%02d{dd}T%02d{hh}:%02d{mm}:%02d{ss}Z\tzscaler_recordid
=%d{recordid}\tsrc_ip=%s{csip}\tsrc_port=%d{csport}\tdst_ip=%s{cdip}\tdst_port=%d{cdport}\tduration=%d{durationms}\tprotocol
=%s{ipproto}\tservice=%s{nsvvc}\trequest_bytes=%ld{outbytes}\tresponse_bytes=%ld{inbytes}
```

---

**User Obfuscation**  
 Enabled  Disabled

---

**Duplicate Logs**  
Disabled

---

**NSS Type**  
 NSS for Web  NSS for Firewall

---

**Status**  
 Enabled  Disabled

---

**SIEM IP Address**  
\_\_\_\_\_

---

**Feed Escape Character**  
\_\_\_\_\_

---

**Timezone**  
GMT

---

| ACTION             | WHO | SOURCE | SERVER | SESSION | PROTOCOL CLASSIFICATION | SECURITY |
|--------------------|-----|--------|--------|---------|-------------------------|----------|
| FIREWALL FILTERS   |     |        |        |         |                         |          |
| DNAT Policy Action |     |        |        |         |                         |          |

Save
Cancel

## Event comparison

Zeek was designed for the express purpose of logging network metadata. In contrast, Zscaler is a cloud-based firewall with logging capabilities.

- [General](#)
- [DNS](#)
- [Flow](#)
- [HTTP](#)
- [SSL](#)

### General

Zscaler events have several differences compared to Zeek events:

|                               |  |
|-------------------------------|--|
| <b>Fewer event types</b>      | We currently only support DNS, Flow, HTTP, and SSL.  |
| <b>Fewer fields</b>           | In general, Zscaler only has a fraction of the fields as Zeek.   |
| <b>Fewer events</b>           | The number of events received depends on how Zscaler is configured. For example, DNS and flow are only available if the firewall feature is used. Even then, the number of events depends on the configuration.                              |
| <b>Different field values</b> | Even when Zscaler has the same field as Zeek, it may not always have the same value. When possible, we convert the values to match Zeek. However, this is difficult to do reliably. In some cases, we are choosing not to do any conversion. |
| <b>No flow ID</b>             | There is no identifier to tie together flow events to the others. It is likely that the flow events that are received are unrelated to the other event types.  |

### DNS

| Field             | Available | Comments   |
|-------------------|-----------|--|
| <b>answers</b>    | Yes       | Zscaler only provides a single answer, not an array like Zeek.                             |
| <b>dst.ip</b>     | Yes       |  |
| <b>dst.port</b>   |           |  |
| <b>flow_id</b>    |           |  |
| <b>proto</b>      |           |  |
| <b>qtype</b>      | Yes       | This is derived from <code>qtype_name</code> , so it may be missing for unexpected values. |
| <b>qtype_name</b> | Yes       |  |
| <b>query</b>      | Yes       |  |
| <b>rcode</b>      | Yes       | This is derived from <code>rcode_name</code> , so it may be missing for unexpected values. |
| <b>rcode_</b>     | Yes       | Zscaler also uses this as an error field, so it may contain unexpected values that are     |

| Field           | Available | Comments        |
|-----------------|-----------|-----------------|
| <b>name</b>     |           | passed through. |
| <b>rejected</b> |           |                 |
| <b>src.ip</b>   | Yes       |                 |
| <b>src.port</b> |           |                 |
| <b>ttls</b>     |           |                 |

## Flow

| Field                 | Available | Comments   |
|-----------------------|-----------|--|
| <b>dst.ip</b>         | Yes       |  |
| <b>dst.ip_bytes</b>   | Yes       |  |
| <b>dst.pkts</b>       |           |  |
| <b>dst.port</b>       | Yes       |  |
| <b>duration</b>       | Yes       |  |
| <b>flow_id</b>        |           |  |
| <b>flow_state</b>     |           |  |
| <b>proto</b>          | Yes       | The values are mostly passed through from Zscaler. Some values will match Zeek and others won't. |
| <b>service</b>        | Yes       | The values are mostly passed through from Zscaler. Some values will match Zeek and others won't. |
| <b>src.ip</b>         | Yes       |  |
| <b>src.ip_bytes</b>   | Yes       |  |
| <b>src.pkts</b>       |           |  |
| <b>src.port</b>       | Yes       |  |
| <b>total_ip_bytes</b> | Yes       |  |
| <b>total_pkts</b>     |           |  |
| <b>upload_percent</b> | Yes       |  |

## HTTP

| Field         | Available | Comments |
|---------------|-----------|----------|
| <b>dst.ip</b> | Yes       |          |

| Field                             | Available | Comments   |
|-----------------------------------|-----------|--|
| <b>dst.port</b>                   |           |  |
| <b>files</b>                      |           |  |
| <b>flow_id</b>                    |           |  |
| <b>headers.accept</b>             |           |  |
| <b>header.content.md5</b>         |           |  |
| <b>headers.content_type</b>       | Yes       | Zscaler may be translating some values into human-readable forms (for example, <i>Flash</i> ). |
| <b>headers.cookie_length</b>      |           |  |
| <b>headers.location</b>           |           |  |
| <b>headers.origin</b>             |           |  |
| <b>headers.proxied_client_ips</b> |           |  |
| <b>headers.refresh</b>            |           |  |
| <b>headers.refresh</b>            |           |  |
| <b>headers.server</b>             |           |  |
| <b>headers.x_powered_by</b>       |           |  |
| <b>host</b>                       |           |  |
| <b>info_msg</b>                   |           |  |
| <b>method</b>                     | Yes       | Zscaler provides a value of <i>CONNECT</i> for <i>HTTPS</i> .                                  |
| <b>referrer</b>                   | Yes       | Zscaler does not provide the scheme (for example., <code>http://</code> ).                     |
| <b>request_len</b>                | Yes       |  |
| <b>request_mime</b>               |           |  |
| <b>request_mimes</b>              |           |  |
| <b>response_len</b>               | Yes       |  |
| <b>response_mime</b>              |           |  |
| <b>response_mimes</b>             |           |  |
| <b>src.ip</b>                     | Yes       |  |
| <b>src.port</b>                   |           |  |
| <b>status_code</b>                | Yes       |  |
| <b>status_msg</b>                 |           |  |

| Field              | Available | Comments |
|--------------------|-----------|----------|
| <b>trans_depth</b> |           |          |
| <b>uri</b>         | Yes       |          |
| <b>user_agent</b>  | Yes       |          |
| <b>username</b>    |           |          |

## SSL

Every HTTPS request will have both an HTTP and SSL event. Unlike Zeek, SSL events are only available for HTTPS. Also, Zscaler documentation suggests that it can be configured to intercept SSL. In that case, the cipher and version field represents the server, which may be different from the values for the client.

| Field                         | Available | Comments  |
|-------------------------------|-----------|---|
| <b>client_issuer</b>          |           |   |
| <b>client_subject</b>         |           |   |
| <b>cipher</b>                 | Yes       | Zscaler values are passed through without conversion since they do not match Zeek.  |
| <b>dst.ip</b>                 | Yes       |   |
| <b>dst.port</b>               |           |   |
| <b>flow_id</b>                |           |   |
| <b>issuer</b>                 |           |   |
| <b>ja3</b>                    |           |   |
| <b>ja3s</b>                   |           |   |
| <b>src.ip</b>                 | Yes       |   |
| <b>src.port</b>               |           |   |
| <b>server_name</b>            | Yes       |   |
| <b>server_name_indication</b> | Yes       |   |
| <b>subject</b>                |           |   |
| <b>session_id</b>             |           |   |
| <b>validation_status</b>      |           |   |
| <b>version</b>                | Yes       | Zscaler values are converted to Zeek, but unexpected values will be passed through. |

## Sensor provisioning

FortiNDR Cloud sensors are self-provisioning appliances that require a registration code from the portal.

### To provision a sensor:

1. [Generate a registration code on page 175](#)
2. [Register a sensor on page 176](#)

Once these steps are complete, the sensor will call home, provision itself, and then be ready to ingest raw mirrored traffic. By default, a sensor will use DHCP but a static IP address can be set if desired.



Each account is limited to ten (10) sensors by default. To expand this limit, contact your Technical Success Manager.

---

## Generate a registration code

Registration codes can be generated on the *Sensors* page within FortiNDR Cloud. If you do not have access to this page, please contact your Fortinet representative.



- Codes expire 24 hours after creation
  - Codes may be used to provision multiple sensors prior to expiration
  - Codes work for both physical and virtual sensors
  - Each account is limited to ten (10) sensors by default. To expand this limit, contact your Technical Success Manager
- 

### To generate a registration code:

1. Click the *Settings* icon at the top right of the page and select *Sensors*. The *Sensors* page opens.



2. In the toolbar, click *Actions > Provision Sensor*. The *New Registration Code* dialog displays a randomly generated registration code prepended with the sensor code for its respective account.
  3. If you have access to multiple accounts, verify that the generated code begins with the three-letter sensor code of the proper account.
  4. [Register the sensor](#).
- 



Be sure to write the code down or copy it locally as it will not be shown again after the pop-up box is closed. If you accidentally close the pop-up box before copying down the code, simply generate another code.

---

## Register a sensor

Registering the sensor takes place within the sensor console. Once registered, the sensor will call home, provision itself, and then be ready to ingest raw mirrored traffic.

See **Verifying Network Connectivity** to troubleshoot connectivity issues.



Registering a sensor requires an Internet connection. Please ensure that the appliance is connected before proceeding.

### To register a sensor:

1. Log in to the sensor console.
2. Select *Provision Sensor* or type `v`.

```
—Main Menu—
(c) Configure Interfaces
(u) Provision Sensor
(t) Test Network
(d) Diagnostics
(p) Set Password

(s) Shutdown Sensor
(r) Reboot Sensor

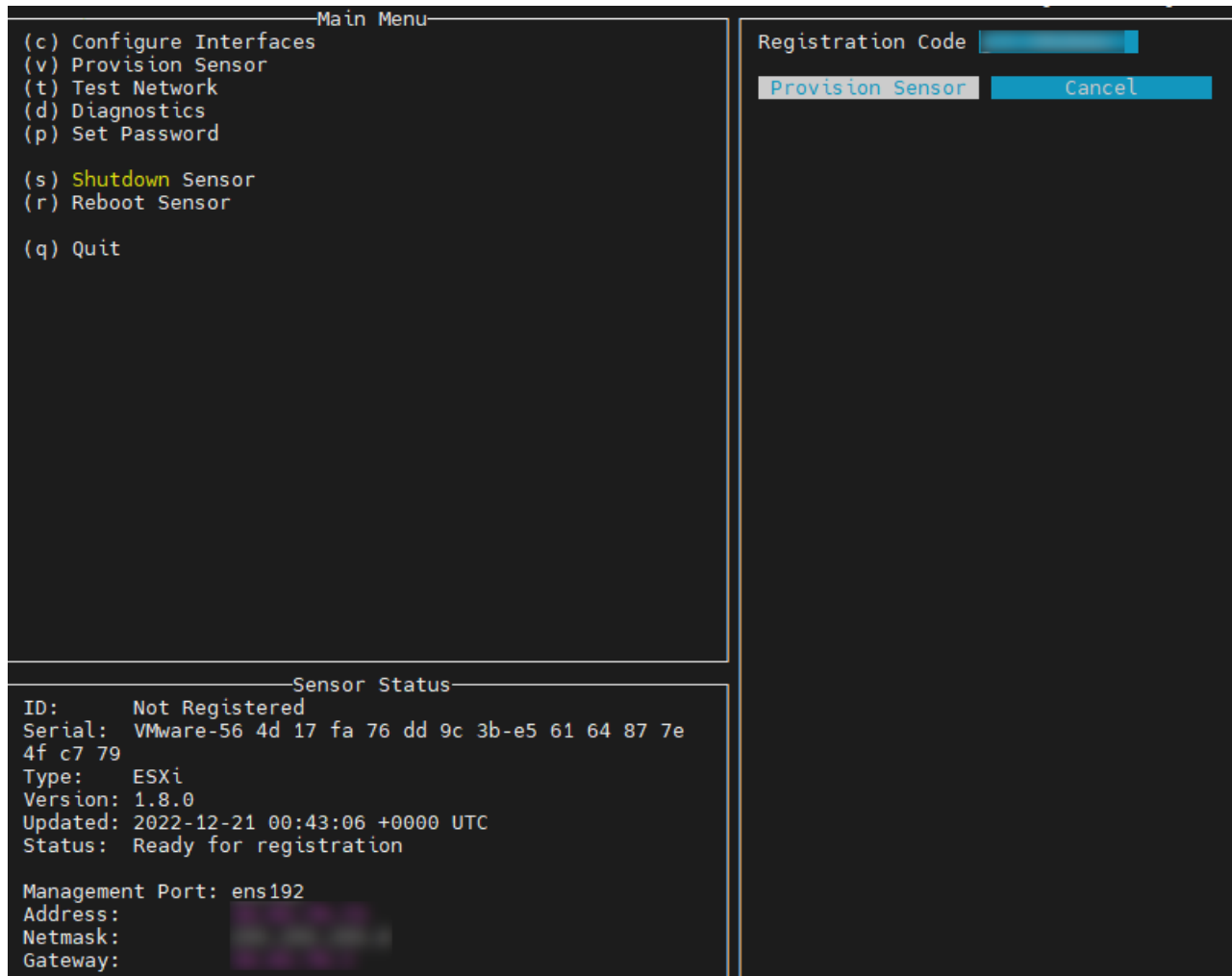
(q) Quit

—Sensor Status—
ID:      Not Registered
Serial:  VMware-56 4d
        17 fa 76 dd 9c 3b-e5 61
        64 87 7e 4f c7 79
Type:    ESXi
Version: 1.8.0
Updated: 2022-12-21
        00:43:06 +0000 UTC
Status:  Ready for
        registration

Management Port: ens192
Address:
10.43.70.73
Netmask:
255.255.255.0
```



3. Enter the registration code in the text box. See [Generate a registration code on page 175](#).



4. Select *Provision Sensor* to begin the registration process. The *Status* changes to *Sensor is provisioning*.
5. Wait for the *Status* to change to *Online*.

## Troubleshooting

### To troubleshoot connectivity issues:

1. Go to *Settings > Sensors*.
2. Click *Visible Devices*.
3. Next to *View*, click *Over Time*.

# FortiNDR Cloud Integrations

FortiNDR Cloud natively supports integrations with multiple security tools and intelligence feeds. It also provides an open framework for creating custom integrations.

The following integrations are currently supported:

|                           |   |
|---------------------------|---|
| <b>SIEM</b>               | <ul style="list-style-type: none"><li>• <a href="#">FortiSIEM</a></li><li>• <a href="#">Splunk</a></li><li>• <a href="#">QRadar</a></li></ul>   |
| <b>SOAR</b>               | <ul style="list-style-type: none"><li>• <a href="#">Cortex-XSOAR</a></li><li>• <a href="#">Splunk SOAR</a></li><li>• <a href="#">FortiSOAR</a></li></ul>  |
| <b>EDR</b>                | <ul style="list-style-type: none"><li>• <a href="#">FortiEDR</a></li><li>• <a href="#">CrowdStrike</a></li></ul>  |
| <b>Intelligence Feeds</b> | <ul style="list-style-type: none"><li>• <a href="#">Proofpoint TAP</a></li><li>• <a href="#">Threat Connect</a></li><li>• <a href="#">CrowdStrike Intel</a></li><li>• <a href="#">Recorded Future Connect</a></li></ul> |

For additional integrations, the SIEM/SOAR integration guide contains details for integrating with other tools. See, [SIEM and SOAR Integration Guide](#).

For network data ingestion, FortiNDR Cloud supports hardware sensors as well as virtual sensors on various platforms, including AWS and ESXi.

- [AWS Sensor Installation Guide](#)
- [ESXi Sensor Installation Guide](#)

FortiNDR Cloud also supports ingesting NSS log data from Zscaler. See, [Zscaler ingestion on page 163](#).

# FortiNDR Cloud APIs

FortiNDR Cloud API documentation is available on the Fortinet Developer Network (FNDN).

## Available APIs

- **Entity API:** Obtain details on individual entities such as IPs, domains, file hashes. This API supports providing details on an entity such as DHCP and DNS information and when it was first and last seen. For information about Entities, see [Entity Panel on page 75](#).
- **Detections API:** Provides details on malicious events that were detected. See [Detections on page 59](#)
- **Sensor API:** Provides APIs for interacting with sensors.
- **Investigations API:** APIs for managing investigations and running queries.

## Metastream

FortiNDR Cloud also provides access to the most recent seven days of events on Metastream. A python client is available to facilitate interacting with the most used events.

- Metastream documentation is available on the Fortinet Developer Network (FNDN).
- Client library documentation is available in the Document library. See, [Metastream Python Library](#).



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.